INFORMATION PROCESSOR COLLECTING AND MANAGING LOG DATA

Publication number: JP10293704 (A)

Publication date: 1998-11-04

Inventor(s): FUJINO SHUJI; MORIKAWA TOSHIYOSHI; URANO AKIHIRO; NAKANO HIDENORI; MORITA SHINJI; YAMADA MITSUGI; NIIMURA YOSHITAKA +

Applicant(s): HITACHI LTD +

Classification:

- **International:** ***G06F11/00; G06F11/34;*** (IPC1-7): G06F11/34
- **European:** G06F11/34T4; H04L12/24A4; H04L12/24D

Application number: JP19970101210 19970418

Priority number(s): JP19970101210 19970418

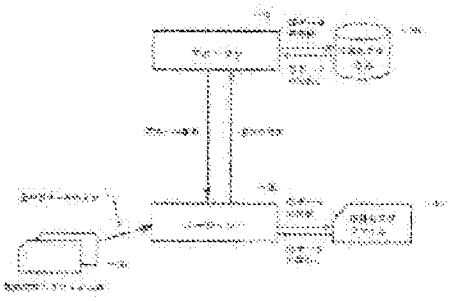
Also published as:

JP3778652 (B2)

US6173418 (B1)

Abstract of **JP 10293704 (A)**

PROBLEM TO BE SOLVED: To manage log data based on a common data format and also to manage log data based on the time of a manager in a system in which a manager collects log data from plural agents through a network. SOLUTION: A manager 10 distributes various rules to an agent 20. The agent 20 inputs log data from a monitored object log file group 30 according to the rules, normalizes it, adds the correction time of a log output time and stores it in a normalization log file 40. The agent 20 fetches normalization log date from the file 40 and transfers it to the manager 10 according to a request from the manager 10. The manager 10 stores collected normalization log data in a normalization log database 50 in order of the correction time.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号

特開平10－293704

(43)公開日　平成10年(1998)11月４日

(51)Int.Cl.[6]	識別記号	Ｆ Ｉ	
Ｇ０６Ｆ　11/34		Ｇ０６Ｆ　11/34	Ｂ

審査請求　未請求　請求項の数５　ＯＬ　（全 24 頁）

(21)出願番号　特願平9－101210

(22)出願日　平成９年(1997)４月18日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　藤野　修司
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　森川　幸義
東京都千代田区大手町二丁目６番２号　株式会社日立情報ネットワーク内

(72)発明者　浦野　明裕
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　高橋　明夫

最終頁に続く

(54)【発明の名称】　ログデータの収集と管理をする情報処理装置

(57)【要約】

【課題】　マネージャがネットワークを介して複数のエージェントからログデータを収集するシステムにおいて、共通的なデータ形式に基づいてログデータを管理する。またマネージャの時刻に基づいたログデータを管理する。

【解決手段】　マネージャ１０は、各種ルールをエージェント２０に配布する。エージェント２０は、このルールに従って監視対象ログファイル群３０からログデータを入力し、正規化し、ログ出力時刻の補正時刻を付加して正規化ログファイル４０に格納する。マネージャ１０からの要求に従ってエージェント２０は、正規化ログファイル４０から正規化ログデータを取り出してマネージャ１０へ転送する。マネージャ１０は、収集した正規化ログデータを補正時刻の順に正規化ログデータベース５０に格納する。

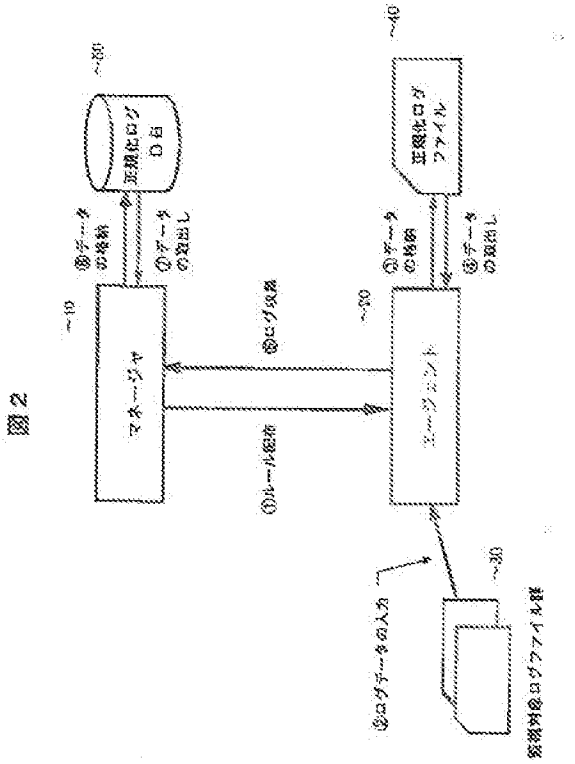


図２

1

【特許請求の範囲】

【請求項１】監視の対象とするログファイル中のログデータからあらかじめ定義されたデータ項目に対応する値を切り出して規定されたデータ項目の値を配列する正規化されたログデータを作成して蓄積する手段と、蓄積された正規化ログデータをネットワークを介してマネージャの機能を実行する情報処理装置へ送信する手段とをエージェントの処理手段として有することを特徴とするログデータの収集をする情報処理装置。

【請求項２】コンピュータ読み取り可能な記憶媒体上に実体化され、ログデータを収集するエージェント機能を有するコンピュータプログラムであって、該プログラムは以下のステップを含む：

（ａ）監視の対象とするログファイル中のログデータからあらかじめ定義されたデータ項目に対応する値を切り出して規定されたデータ項目の値を配列する正規化されたログデータを作成し、（ｂ）蓄積された正規化ログデータをネットワークを介してマネージャの機能を実行するコンピュータへ送信する。

【請求項３】ネットワークを介してエージェントの機能を実行する情報処理装置からあらかじめ定義された共通のデータ形式に従って正規化されたログデータであってマネージャの基準とする時刻に基づいて補正されたログ出力時刻を有する正規化ログデータを受信する手段と、該正規化ログデータを補正時刻の順にデータベースに蓄積する手段とをマネージャの処理手段として有することを特徴とするログデータの収集と管理をする情報処理装置。

【請求項４】該補正時刻とマネージャの現在時刻との差分の時間が所定の保存期間を超過している正規化ログデータを該データベースから削除する手段をさらに設けることを特徴とする請求項３記載のログデータの収集と管理をする情報処理装置。

【請求項５】コンピュータ読み取り可能な記憶媒体上に実体化され、ログデータの収集と管理をするマネージャ機能を有するコンピュータプログラムであって、該プログラムは以下のステップを含む：

（ａ）ネットワークを介してエージェントの機能を実行するコンピュータからあらかじめ定義された共通のデータ形式に従って正規化されたログデータであってマネージャの基準とする時刻に基づいて補正されたログ出力時刻を有する正規化ログデータを受信し、（ｂ）該正規化ログデータを補正時刻の順にデータベースに蓄積する。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、マネージャがネットワークを介してエージェントからログデータを収集するシステムに係わり、特にマネージャがシステム内に存在するログデータを共通的なログデータ形式に基づいて管理するログデータの収集と管理の方式に関する。

2

【０００２】

【従来の技術】情報処理装置で実行されるオペレーティングシステム（ＯＳ）やアプリケーションプログラムは、各種のログ情報を出力する。出力されたログ情報を収集するいくつかの方式が知られている。例えば特開平５－２５０２２９号公報は、複数のコンピュータからのログデータ収集において、ログデータ中のエラーコードを検出することにより、エラー状態のコンピュータからのログデータを優先的に送信するログデータ収集方式を開示する。また特開平５－２８００８号公報は、情報処理システムが障害ログを収集するとき貯蔵手段に貯えられたログ情報の個数が一定数に達したことを検出し、ログ登録の抑止を行うことにより重要な障害情報の消失を防ぐログ情報収集方式を開示する。また特開平５－１１１０２９号公報は、下位の設備端末からのデータが採取された時刻をデータに付与して上位の制御装置に送ることにより、複数の端末からの各データの時系列的な関係が損なわれることがないようにするデータ収集方式を開示する。

【０００３】

【発明が解決しようとする課題】ネットワークを介して複数のコンピュータが接続され、コンピュータが他のコンピュータと通信しながら処理を進める分散処理システムにおいて、一人のユーザは複数の広範囲にわたるコンピュータやファイルにアクセスし得る。従ってログデータを解析することによってコンピュータやファイルへの不正なアクセスを検出するためには、個々のコンピュータが出力するログデータを中央のコンピュータに集約し、データベースに蓄積する必要がある。しかしながら各種のシステムプログラムやアプリケーションプログラムが出力するログデータは、各々そのデータ形式が異なっているので、単に個々のコンピュータプログラムが出力するログデータを収集して集約するだけではログデータの解析が困難である。また個々のコンピュータが保有する時刻がすべてのコンピュータに亘って一致しているとは限らないので、一般に個々のログデータに付与されている時刻にはずれが生じており、集約されたログデータを正しい時刻の順序に従って配列することが困難である。

【０００４】本発明は、上記の事情に鑑みてなされたものであり、その目的とするところは、共通的なデータ形式に正規化されたログデータを管理することにある。

【０００５】本発明の他の目的は、各サイトのコンピュータからログデータを収集する中央のコンピュータの時刻を基準とするログデータを管理することにある。

【０００６】

【課題を解決するための手段】上記目的を達成するため、本発明は、監視の対象とするログファイル中のログデータからあらかじめ定義されたデータ項目に対応する値を切り出して規定されたデータ項目の値を配列する正規化されたログデータを作成して蓄積する手段と、蓄積

された正規化ログデータをネットワークを介してマネージャの機能を実行するコンピュータへ送信する手段とをエージェントの処理手段として有するログデータの収集をするコンピュータを特徴とする。

【０００７】また本発明は、ネットワークを介してエージェントの機能を実行するコンピュータからあらかじめ定義された共通のデータ形式に従って正規化されたログデータであってマネージャの基準とする時刻に基づいて補正されたログ出力時刻を有する正規化ログデータを受信する手段と、該正規化ログデータを補正時刻の順にデータベースに蓄積する手段とをマネージャの処理手段として有するログデータの収集と管理をするコンピュータを特徴とする。

【０００８】

【発明の実施の形態】以下、本発明の一実施形態について図面に基づいて詳細に説明する。

【０００９】図１は、本発明を適用する通信ネットワークの一例を示すシステム構成図である。ネットワークは複数のＬＡＮ１，３，４及びＷＡＮ（ワイド・エリア・ネットワーク）２に結合されるものである。マネージャ１０は、計算機の主記憶装置に格納され、ＯＳの下で走行するアプリケーションプログラム（ＡＰ）である。エージェント２０は、サーバ等の計算機の主記憶装置に格納され、ＯＳの下で走行するＡＰである。マネージャ１０は、ＬＡＮ１，３，４又はＷＡＮ２を介してエージェント２０－１，２０－２，２０－３，２０－４と通信することが可能である。図に示すように、エージェント２０を実行する計算機はエージェント２０と並行して他のＡＰを実行することが可能である。マネージャ１０を実行する計算機もマネージャ１０と並行して他のＡＰを実行することが可能であるが、充分なＣＰＵ性能と資源を確保するためには、専用の計算機を割り当てるのが望ましい。６０はこのネットワークシステムを管理するネットワーク管理システムであり、ネットワーク管理プログラム及び図示しないネットワーク監視端末から構成される。ネットワーク管理システム６０は、ネットワーク資源についての情報をマネージャ１０に提供する。

【００１０】図２は、マネージャとエージェントが行う処理動作の概略を示す図である。マネージャ１０は、定義された各種ルールをエージェント２０へ配布する(①)。エージェント２０は、受信したルールを登録し、そのルールに従い監視対象ログファイル群３０からログデータを入力し(②)、ログデータを正規化した後、正規化ログファイル４０に格納する(③)。このとき正規化ログデータ中のログ出力時刻をマネージャ１０の時刻を基準とする補正時刻によって補正する。エージェント２０

は、マネージャ１０からログ収集要求があったとき正規化ログファイル４０から正規化されたログデータを取り出し(④)、マネージャ１０へ転送する(⑤)。マネージャ１０は、収集した正規化ログデータを補正時刻の順に正規化ログデータベース５０に格納する(⑥)。またマネージャ１０は、必要に応じて正規化ログデータベース５０から任意の正規化ログデータを抽出し、その解析を行う。

【００１１】図３は、マネージャ１０の構成を示す機能ブロック図である。ルール１１０は定義された各種ルールであり、記憶装置に格納される。正規化ログデータベース５０は、収集された正規化ログデータを格納するデータベースであり、記憶装置に格納される。ネットワーク管理システム６０は、ネットワークを介してマネージャ１０を格納する計算機と接続される他の計算機およびネットワークを監視する端末装置から構成されるシステムであり、マネージャ１０と同じ計算機で走行するネットワーク管理プログラムは、ネットワークの構成要素である各通信回線、ルータ、中継機、各種計算機、計算機のプログラム等の動作状態（接続中／接続断、動作中／停止状態など）、各ネットワーク構成要素の所在場所などを管理する。以下マネージャ１０を構成する各機能モジュールの機能の概略について述べる。

【００１２】（１）ルール定義１００

運用者が各種ルールを定義するためのプログラムツールであり、図示しない入力装置及び表示装置を介してユーザが容易にルールを設定できるようなＧＵＩ（グラフィカル・ユーザ・インタフェース）を提供する。

【００１３】（２）スケジューラ１０１

ルール配布及びログ収集を実行する契機をそれぞれルール配布１０６及びログ収集１０７に知らせるプログラムである。契機の例として、例えば毎日午後５時、毎週土曜日の午後３時１５分などのように実行開始を指示する。

【００１４】（３）プロセス管理１０２

マネージャ１０の１００～１０９を付す各機能モジュールの起動／停止を制御するプログラムである。

【００１５】（４）ログ解析１０３

データベース管理１０９を介して正規化ログデータベース５０から正規化ログデータ群を抽出し、所定の解析を行うプログラムである。以下ログ事象がログインである場合のログデータ解析の例を表１に示す。ログ事象及び正規化項目については後述する。

【００１６】

【表１】

ログデータ解析の例（表１）

ログ解析項目	使用する正規化項目
規定のログイン地域でない所からログインし成功した	ユーザ名 接続元ホスト名 接続元ＩＰアドレス
規定の時間外にログインして失敗した	ユーザ名 開始時刻
同一ユーザが別々の地域から同時にログインしている	ユーザ名 接続元ホスト名
一定期間に規定回数以上のログイン回数がありログインに失敗した	ログ事象 ログ事象結果 ユーザ名 補正時刻
規定回数以上、ユーザ名とパスワードの組み合わせを失敗したユーザ変更を行った	ログ事象 ログ事象結果 ユーザ名 変更後のユーザ名 補正時刻

【００１７】（５）構成管理１０４
対象とするエージェント２０の一覧を管理するプログラムである。またネットワーク管理システム６０に問い合わせを行ってエージェント２０が動作する計算機の動作有無やｐｉｎｇの応答時間等の情報を取得してルール配布１０６又はログ収集１０７に渡す。
【００１８】（６）ルール管理１０５
ルール定義１００から定義された各種ルールを受け取ってルール１１０に格納する。またルール１１０からルールを読み出してルール配布１０６に渡す。
【００１９】（７）ルール配布１０６
スケジューラ１０１の指示に従い、ルール管理１０５から各種ルールを取得してエージェント２０へ配布するプログラムである。
【００２０】（８）ログ収集１０７
スケジューラ１０１の指示に従い、エージェント２０から正規化ログファイルを収集するプログラムである。
【００２１】（９）データ通信１０８
ルール配布１０６及びログ収集１０７がエージェント２０と通信するときに通信制御を行うプログラムである。
【００２２】（１０）データベース管理１０９
ログ収集１０７がエージェント２０から収集した正規化ログデータ群（正規化ログファイル）を正規化ログデータベース５０に格納し、ログ解析１０３からの要求によって正規化ログデータを検索し抽出する。また所定の保存期間を過ぎた正規化ログデータを正規化ログデータベース５０から削除し、未使用の記憶領域を生み出す。
【００２３】図４は、エージェント２０の構成を示す機能ブロック図である。ルール２０５は配布を受けた各種ルールであり、記憶装置に格納される。監視対象ログファイル群３０は、監視対象とするログファイルであり、記憶装置に格納される。正規化ログファイル４０は、正規化ログデータを格納するファイルであり、記憶装置に格納される。以下エージェント２０を構成する各機能モジュールの機能の概略について述べる。
【００２４】（１）データ通信２００
データ通信２００は、ルール管理２０３及びログファイル管理２０４がマネージャ１０と通信するときに通信制御を行うプログラムである。
【００２５】（２）プロセス管理２０１
エージェント２０の２００～２０４を付す各機能モジュールの起動／停止を制御するプログラムである。
【００２６】（３）ログ入力２０２
ルール管理２０３からログファイル監視ルールやフォーマットルール等を取得し、監視対象ログファイル群３０から入力したログデータを正規化した後、正規化ログデータをログファイル管理２０４へ渡すプログラムである。
【００２７】（４）ルール管理２０３
マネージャ１０から配布された各種ルールをルール２０５として記憶装置に格納し、ログ入力２０２又はログファイル管理２０４の要求に応じてルールを提供するプログラムである。
【００２８】（５）ログファイル管理２０４
ルール管理２０３からフィルタリングルールを取得し、ログ入力２０２から受け取った正規化ログデータをフィルタリングし、補正時刻を付加して正規化ログファイル４０に格納する。マネージャ１０のログ収集１０７から正規化ログファイル４０の収集要求を受けたとき、正規化ログファイル４０をマネージャ１０へ転送する。
【００２９】図５～図１４は、正規化ログデータの構造の一例を示す図である。

7

【００３０】図５は、正規化ログファイル４０に格納される正規化ログデータ３００の概略構成を示す図である。正規化ログデータ３００は、共通情報クラス３０１と必要に応じて追加されるユーザ情報クラス３０２、サービス情報クラス３０３、アドレス情報クラス３０４、ファイル情報クラス３０５、トラフィク情報クラス３０６、個別情報クラス３０７等から構成される。共通情報クラス３０１は、すべての正規化ログデータ３００に必須の情報クラスであり、残りの情報クラスは出力されたログデータに応じて選択されるものである。

【００３１】図６は、共通情報クラス３０１のデータ構成を示す図である。正規化バージョン３１０は、正規化のバージョンを示す番号である。ログ種別はログ事象３１１、ログ事象結果３１２、ログ出力プログラム３１３、データ格納クラス３１４及びログファイル名３１５を含む。ログ出力プログラム３１３はログを出力したＯＳ又はＡＰの名称であり、ログファイル名３１５はログ出力プログラム３１３が出力したログファイルの名称である。ログ事象３１１、ログ事象結果３１２及びデータ格納クラス３１４については後述する。マネージャは、マネージャを搭載する計算機のホスト名３１６とホストＩＰアドレス３１７を格納する。エージェントは、ログを入力したエージェントを搭載する計算機のホスト名３１８とホストＩＰアドレス３１９を格納する。監視対象は、監視対象とするサーバ等の計算機のホスト名３２０とホストＩＰアドレス３２１を格納する。時刻はログ出力時刻３２２と補正時刻３２３から成る。ログ出力時刻３２２はログを出力した計算機の局所的な時刻であり、補正時刻３２３はマネージャ１０を搭載する計算機の時刻に基づいて補正した時刻である。フィルタリングルール名３２４は、ログデータを正規化するときに適用したフィルタリングルールの名称である。

【００３２】図７は、ユーザ情報クラス３０２のデータ構成を示す図である。ユーザ情報クラス３０２は、ログインしたユーザに関する情報を記録するものであり、ユーザ名３３０、ユーザＩＤ（ＵＩＤ）３３１、ユーザ変更した後のユーザ名３３２、変更後のＵＩＤ３３３、ユーザのセキュリティレベル３３４、計算機やファイルへのアクセス権３３５、アクセスした結果３３６及びユーザが操作した端末装置の名称（端末名３３７）を格納する。

【００３３】図８は、サービス情報クラス３０３のデータ構成を示す図である。サービス情報クラス３０３は、ユーザに提供したサービスについての情報を記録する。サービスは、サービス名３４０、サービスバージョン３４１、サービス提供のために起動したプロセスの名称（プロセス名３４２）及びプロセスＩＤ３４３を格納する。

【００３４】図９は、アドレス情報クラス３０４のデータ構成を示す図である。アドレス情報クラス３０４は、

8

他計算機とコネクションを行ったときの情報を記録するものであり、接続元及び接続先のホスト名、ＩＰアドレス、ＭＡＣアドレス、ポート番号の他にコネクション状態、コネクションの開始時刻と終了時刻及び他計算機へのアクセス結果を格納する。

【００３５】図１０は、ファイル情報クラス３０５のデータ構成を示す図である。ファイル情報クラス３０５は、ユーザが作成又は変更したファイルについてファイル名、変更前のアクセス情報及び変更後のアクセス情報を記録する。アクセス情報は、ファイルの作成時刻、最終修正時刻、最終アクセス時刻、ファイルのｉ－ｎｏｄｅ番号、アクセス許可の有無、ＵＩＤ、グループＩＤ（ＧＩＤ）及び最終的なファイルのサイズを格納する。

【００３６】図１１は、トラフィク情報クラス３０６のデータ構成を示す図である。トラフィク情報クラス３０６は、メール管理プログラム、ファイル転送プログラム等が出力するログ情報であり、ネットワークを介するデータやメッセージの受信バイト数、送信バイト数及びデータの転送時間（処理時間）を記録する。

【００３７】図１２は、個別情報クラス３０７のデータ構成を示す図である。個別情報クラス３０７は、オプションであり、プログラムが出力するメッセージテキストの原文そのままの情報である。

【００３８】図１３は、データ格納クラス３１４のデータ構造を示す図である。“Ｔ１”はデータ格納クラス３１４を識別するためのタグであり、“Ｌ１”は存在する情報クラスを指定する領域Ｖ１の長さを示す。“Ｖ１”は、各正規化ログデータ３００に含まれる情報クラスを指定する領域であり、情報クラスの指定の開始を示すタグ、情報クラス識別子の長さ及び情報クラス識別子を順番に指定する。情報クラス識別子の長さは可変長である。各情報クラスを識別する番号をｘとすると、Ｔｘ（ｘ≧２）は情報クラスの開始を示すタグであり、Ｌｘ（ｘ≧２）はそのＶｘの部分の長さであり、Ｖｘ（ｘ≧２）は情報クラス識別子である。マネージャ１０は、このデータ格納クラス３１４により各正規化ログデータが有する情報クラスを認識する。

【００３９】図１４は、正規化項目のうちコード化が可能なもののコード化テーブル６００の一例を示す図である。正規化項目のログ事象３１１が“ｌｏｇｉｎ”の場合はコード“１”に、ユーザ変更“ｓｕ”の場合はコード“２”というようにコード化される。コネクト（ｃｏｎｎｅｃｔ）は、計算機間でファイル転送やプログラム間通信を行う際のコネクションに関するログ事象を示す。ファイルは内容変更されたファイルに関するログ事象、ジョブはジョブの起動／停止／終了状態に関するログ事象である。メールはメール使用に関するログ事象を示す。ログ事象結果３１２はログ事象の結果であり、成功か失敗かを区分する。ユーザ情報クラス３０２のアクセス権３３５についてはあり又はなしを区分する。ユー

9

ザ情報クラス３０２及びアドレス情報クラス３０４のアクセス結果については、成功か失敗かを区分する。ファイル情報クラス３０５のアクセス許可については、あり又はなしを区分する。

【００４０】図１５～図２０は、ルールのデータ形式を示す図である。

【００４１】図１５は、マネージャルール４５０の一例を示す図である。ＤＢ＿ＭＡＸ４５１は正規化ログデータベース５０が正規化ログデータを保存可能な期間を示す保存期間を定義する。ＲＵＩＥ＿ＭＡＸ４５２はルール配布に使用できる最大の通信路数を定義する。ＬＯＧ＿ＭＡＸ４５３はログ収集に使用できる最大の通信路数を定義する。ルール配布１０６やログ収集１０７は、この多重度数だけ通信路を使用できるか、処理の要求がこの多重度より大きい場合は通信路を順番に使用し、通信路が空くまで待った後、残りの処理を実行する。

【００４２】図１６は、エージェント２０の動作条件ルール４７０の一例を示す図である。ＭＡＮＡＧＥＲ＿ＡＤＤＲＥＳＳ４７１はマネージャのＩＰアドレスを定義し、ＦＩＬＥ＿ＭＡＸＳＩＺＥ４７２は正規化ログファイル４０が使用できる最大の記憶容量を定義する。

【００４３】図１７は、ログファイル監視ルール５００の一例を示す図である。ＴＡＲＧＥＴ＿ＬＯＧは監視対象ログファイル名を定義し、ＦＯＲＭＡＴによりファイルの形式（ＳＥＱ：シーケンシャル形式、ＷＲＡＰ：ラップアラウンド形式）を定義し、ＩＮＴＥＲＶＡＬにより監視間隔の時間（たとえば、１０分間隔）を定義する。ＦＭＴ＿ＮＡＭＥは当該ログファイルを正規化するときに適用するルールを定義する。例により説明すると、

TARGET_LOG:/usr/adm/syslog.log,FORMAT=SEQ,INTERVAL=10m,FMT_NAME=abc;

は、シーケンシャル形式のファイル／ｕｓｒ／ａｄｍ／ｓｙｓｌｏｇ．ｌｏｇを１０分間隔で監視し、フォーマットルールａｂｃにより正規化処理を行うことを示す。ＦＭＴ＿ＮＡＭＥの指定がない場合は、エージェント２０の間で共通のフォーマットルールにより正規化を行う。

【００４４】図１８と図１９は、フォーマットルール５１０及び５１５の一例を示す図である。ログデータがテキスト形式の場合はＦＭＴ＿Ｔを適用し、バイナリ形式の場合はＦＭＴ＿Ｂを適用する。ＲＥＧＴＥＸＴ＝“文字列ｎ”は、ログデータを選択する条件を示し、ログデータ中に文字列ｎが存在すれば、以下に示す規則に従ってログデータを正規化することを示す。＆＆は論理積（ＡＮＤ）を示し、複数の文字列の存在を選択条件とすることができる。：はｔｈｅｎを意味し、以下ログデータの文字列のシーケンスに従って文字列から順に正規化項目を拾って行くことを意味する。正規化項目とは、各情報クラスで定義されるデータ項目のことである。：

10

は、ログデータの先頭から順番にポインタをずらして正規化項目に対応する値を切り出すための区切り文字である。正規化項目に続いて［］内に指定される文字は、任意のポインタから認識する文字列の長さ、またはその文字列が可変長の場合に認識する最後の文字を指定する。ＳＫＩＰは、ログデータの先頭から順番にポインタをずらしていった場合、正規化項目に関係ない文字列が存在する場合にその文字列を読み飛ばすことを意味し、［］内には読み飛ばす文字数又は認識する最後の文字となる“区切り文字”を指定する。区切り文字を指定した場合は、その区切り文字まで読み飛ばす。以下フォーマットルールの例を挙げる。

（ａ）フォーマットルールＡ

FMT_T:REGTEXT == "SU" && REGTEXT == "+" | ログ事象 == "2" | ログ事象結果== "0" :SKIP[" "]:ログ出力時刻[10]: SKIP[3]:端末名[" "]:ユーザ名["-"]:変更後のユーザ名[" "];

（ｂ）フォーマットルールＢ

FMT_T:REGTEXT == "connect" && REGTEXT == "refused" | ログ事象 == "3" | ログ事象結果 == "1" :ログ出力時刻[15]: 接続先ホスト名[" "]:プロセス名["["]:プロセスＩＤ["]"]:SKIP["from "]:接続元ホスト名[" "];

図２１は、ログファイルに格納されているメッセージテキストの原文の例を示す図である。メッセージテキスト５５１及び５５２は、ＯＳが出力するユーザ変更に関するメッセージテキストの例である。メッセージテキスト５５３～５５５は、ＯＳがコネクション時に出力するメッセージテキストである。メッセージテキスト５５６及び５５７は、ＯＳのジョブ管理が出力するメッセージテキストである。

【００４５】メッセージテキスト５５１をフォーマットルールＡによって正規化すると、

・ログ事象３１１＝２（ｓｕ）
・ログ事象結果３１２＝０（成功）
・ログ出力時刻３２２＝１／３０　１１：１８のエポックタイム
・端末名３３７＝ｔｙｐ５
・ユーザ名３３０＝ｆｕｊｉｎｏ
・変更後のユーザ名３３２＝ｒｏｏｔ

となる。

【００４６】メッセージテキスト５５４をフォーマットルールＢによって正規化すると、

・ログ事象３１１＝３（ｃｏｎｎｅｃｔ）
・ログ事象結果３１２＝１（失敗）
・ログ出力時刻３２２＝Ｊａｎ　１２　１３：１２：１５のエポックタイム
・接続先ホスト名３５４＝ｈｏｓｔａ
・接続先ＩＰアドレス３５５＝ｈｏｓｔａをＩＰアドレスに変換した値

11

・プロセス名３４２＝ｆｔｐｄ
・プロセスＩＤ３４３＝１１１１
・接続元ホスト名３５０＝ｈｏｓｔｂ
・接続元ＩＰアドレス３５１＝ｈｏｓｔｂをＩＰアドレスに変換した値
となる。

【００４７】図２０は、フィルタリングルール６２０の一例を示す図であり、ログファイル管理２０４が該当する正規化ログデータだけを格納するためのルールである。ＦＬＴはフィルタリングルールであることを示し、正規化項目が指定した文字列やコードであったり、指定した時間帯の正規化ログデータであった場合、そのような条件に適合する正規化ログデータだけを抽出して格納する。＝＝はイコールを、！＝はｎｏｔイコールを、＆＆は論理積ＡＮＤを、｜｜は論理和ＯＲを、－は時間間隔をそれぞれ意味する。

【００４８】図２２は、正規化ログデータベース５０のデータ構造を例示する図である。正規化ログデータベース５０は、正規化ログデータを補正時刻６３０の順に配列して格納する。ある補正時刻６３０から共通情報クラス６３１のログデータにチェインする。また共通情報クラス６３１からこれに続いて存在する情報クラスのログデータに次々とチェインする。情報クラスに対応して示される検索キーは、正規化ログデータを検索するときにキーとして使用される正規化項目を示すものである。また補正時刻６３０から次の補正時刻６３０へチェインが張られている。ユーザは、補正時刻６３０によって、また該当する情報クラスの検索キーを指定することによって正規化ログデータベース５０から目的とする正規化ログデータを効率良く抽出することができる。

【００４９】図２３は、マネージャ１０のルール配布１０６の処理の流れを示すＰＡＤ図である。ルール配布１０６は、初期設定（ステップ７０１）後、プロセス管理１０２から終了要求が来るまでループし（ステップ７０２）、イベントを待つ（ステップ７０３）。イベントには、スケジューラ１０１からのルール配布要求（ステップ７０４）とプロセス管理１０２からの終了要求（ステップ７１２）がある。

【００５０】ルール配布要求（ステップ７０４）を受信した場合は、ルール管理１０５を介して配布するルールと配布先であるエージェント２０の一覧を取得し（ステップ７０５）、構成管理１０４からエージェント２０の動作状態及び応答時間の情報を取得する（ステップ７０６）。取得したエージェント２０のｐｉｎｇ応答時間を応答時間の小さい順番に並べ替える（ステップ７０７）。このとき動作していないエージェント２０については、応答時間を無限大と解釈する。ルールを配布するエージェント２０の数だけループし（ステップ７０８）、エージェント２０が動作している場合（ステップ７０９ＹＥＳ）は応答時間の小さい順番にルールを配布

12

し（ステップ７１０）、エージェント２０が動作していない場合はルール配布失敗のメッセージを出力する（ステップ７１１）。ルール配布に当っては、ＲＵＬＥ＿ＭＡＸ４５２を適用する。配布したルールは、エージェント２０のルール管理２０３に転送される。

【００５１】終了要求を受信した場合は（ステップ７１２）、ループを抜けて終了処理を行う（ステップ７１３）。

【００５２】図２４は、マネージャ１０のログ収集１０７の処理の流れを示すＰＡＤ図である。ログ収集１０７は、初期設定（ステップ８０１）後、プロセス管理１０２から終了要求が来るまでループし（ステップ８０２）、イベントを待つ（ステップ８０３）。イベントには、スケジューラ１０１からのログ収集要求（ステップ８０４）、エージェント２０からの起動通知（ステップ８１１）、及びプロセス管理１０２からの終了要求（ステップ８１６）がある。

【００５３】ログ収集要求を受信した場合は（ステップ８０４）、スケジューラ１０１からログを収集するエージェント２０の一覧を取得し（ステップ８０５）、構成管理１０４からこれらのエージェント２０の動作状態及び応答時間の情報を取得するとともに、応答時間の短い順番にエージェント２０をソートする（ステップ８０６）。ログを収集するエージェント２０の数分ループし（ステップ８０７）、エージェントが動作している場合（ステップ８０８ＹＥＳ）はログを収集し（ステップ８０９）、エージェントが動作していない場合（ステップ８０８ＮＯ）はログ収集失敗メッセージを出力する（ステップ８１０）。ログ収集に当っては、ＬＯＣ＿ＭＡＸ４５３を適用する。ログ収集１０７は、エージェント２０のログファイル管理２０４を介して正規化ログファイル４０を収集する。

【００５４】エージェント起動通知を受信した場合は（ステップ８１１）、構成管理１０４からエージェント２０とのｐｉｎｇ（ＩＣＭＰエコーリクエスト）の応答時間を取得する（ステップ８１２）。ＩＣＭＰ（Ｉｎｔｅｒｎｅｔ ＣｏｎｔｒｏｌＭｅｓｓａｇｅ Ｐｒｏｔｏｃｏｌ）は、通信ネットワークの管理に関する国際的な標準規格の１つであるアイ・エイ・ビー（ＩＡＢ：Ｉｎｔｅｒｎｅｔ ＡｃｔｉｖｉｔｌｅｓＳ Ｂｏａｒｄ）の管理標準である。ＩＣＭＰを使用すると、ＩＰノード（例えばコンピュータ）が他のＩＰノードと通信可能であるか否かを確認できる。またｐｉｎｇを使用すると、任意のＩＰノードと通信可能であるか否かの動作状態と応答時間を取得できる。ｐｉｎｇ応答時間を取得できた場合（ステップ８１３ＹＥＳ）は、マネージャ１０の現在時刻にこの応答時間から得られる通信往時間を加算した時刻を起動通知を発行したエージェント２０へ通知する（ステップ８１４）。マネージャの時刻をエージェントに伝えるためには、マネージャの時刻にマネージャから

エージェントへの通信時間を加えた時刻を通知すればよい。ｐｉｎｇの応答時間は、マネージャからエージェントとエージェントからマネージャ、つまり行きと返りの通信時間を加えた時間間隔である。そこでｐｉｎｇ応答時間の１／２を通信時間として利用する。すなわちマネージャは、次の計算式によりエージェントの時刻を推定しエージェントへ通知する。

（エージェントの時刻）≒（マネージャの時刻）＋（ｐｉｎｇ応答時間）／２

応答時間を取得できなかった場合（ステップ８１３ＮＯ）、すなわちネットワーク管理システム６０から情報を得られない場合は、単にマネージャ１０の現在時刻をエージェント２０へ通知する（ステップ８１５）。エージェント２０は、マネージャ１０の現在時刻を取得して正規化ログデータの補正時刻３２３に適用する。

【００５５】終了要求を受信した場合は（ステップ８１６）、ループを抜けて終了処理を行う（ステップ８１７）。

【００５６】図２５は、マネージャ１０の構成管理１０４の処理の流れを示すＰＡＤ図である。構成管理１０４は、初期設定（ステップ９０１）後、プロセス管理１０２から終了要求が来るまでループし（ステップ９０２）、イベントを待つ（ステップ９０３）。イベントにはルール配布１０６からのエージェント情報格納要求（ステップ９０４）、ルール配布１０６やログ収集１０７からのエージェント情報取得要求（ステップ９０９）と、プロセス管理１０２からの終了要求（ステップ９１３）がある。

【００５７】エージェント情報格納要求を受信した場合は（ステップ９０４）、ルール配布１０６からルールを配布したエージェント２０の情報を取得する（ステップ９０５）。エージェント２０の情報とは、ルールの配布時刻、配布したルール名などである。ネットワーク管理システム６０と通信可能であるとき（ステップ９０６ＹＥＳ）は、取得したエージェント情報をネットワーク管理システム６０に渡す（ステップ９０７）。ネットワーク管理システム６０は、受信したルール配布の履歴情報をネットワーク管理のために利用可能である。ネットワーク管理システム６０と通信できないとき（ステップ９０６ＮＯ）は、エージェント情報を構成管理１０４が保有するファイルへ格納する（ステップ９０８）。

【００５８】エージェント情報取得要求を受信した場合は（ステップ９０９）、ネットワーク管理システム６０と通信できるとき（ステップ９１０ＹＥＳ）には、ネットワーク管理システム６０からエージェント２０の一覧、動作有無やｐｉｎｇの応答時間等を取得しこれらの情報を要求元に返す（ステップ９１１）。ネットワーク管理システム６０と通信できないとき（ステップ９１０ＮＯ）には、構成管理１０４のファイルからエージェントの一覧についての情報を取得して要求元に返す（ステップ９１２）。

【００５９】終了要求を受信した場合は（ステップ９１３）、ループを抜けて終了処理（ステップ９１４）を行う。

【００６０】図２６は、マネージャ１０のデータベース管理１０９の処理の流れを示すＰＡＤ図である。データベース管理１０９は、初期設定（ステップ１００１）し、正規化ログデータベース５０に格納している正規化ログデータの保存期間の確認を要求（ステップ１００２）した後、プロセス管理１０２から終了要求が来るまでループし（ステップ１００３）、イベントを待つ（ステップ１００４）。イベントには、ログ収集１０７からの正規化ログデータ格納通知（ステップ１００５）、ログ解析１０３からの正規化ログデータ抽出要求（ステップ１００８）、データベース管理１０９自身が正規化ログデータの保存期間を確認するための要求（ステップ１０１０）と、プロセス管理１０２からの終了要求（ステップ１０１４）がある。

【００６１】正規化ログデータ格納通知を受けた場合は（ステップ１００５）、ログ収集１０７から正規化ログデータを取得し正規化ログデータベース５０に格納する（ステップ１００６）。格納に当っては、図２２のデータ構造に従って正規化ログデータを格納する。正規化ログデータは補正時刻６３０の順に配列されるので、この順に従って正規化ログデータをマージする。また正規化ログデータの保存期間確認を要求する（ステップ１００７）。

【００６２】正規化ログデータ抽出要求を受信した場合は（ステップ１００８）、指定された検索キーにより正規化ログデータベース５０を検索し、その結果抽出したデータを要求元へ応答する（ステップ１００９）。

【００６３】保存期間確認要求（ステップ１０１０）を受信した場合は、正規化ログデータベース５０に格納されている正規化ログデータの一番古い補正時刻６３０と現在時刻の差と、ＤＢ＿ＭＡＸ４５１とを比較し（ステップ１０１１）、保存期間より古い正規化ログデータを保存しているときは古い正規化ログデータを削除し（ステップ１０１２）、運用者に知らせるために削除メッセージを出力する（ステップ１０１３）。

【００６４】終了要求を受信した場合は（ステップ１０１４）、ループを抜けて終了処理（ステップ１０１５）を行う。

【００６５】図２７は、エージェント２０のログ入力２０２の処理の流れを示すＰＡＤ図である。ログ入力２０２は、初期設定し（ステップ１１０１）、エージェント２０のルール管理２０３からログファイル監視ルール５００とフォーマットルール５１０，５１５等を取得（ステップ１１０２）後、プロセス管理２０１から終了要求が来るまでループし（ステップ１１０３）、イベントを待つ（ステップ１１０４）。イベントには、ログファイ

15

ル管理２０４からのログ入力中断要求（ステップ１１０５）とログ入力再開要求（ステップ１１０７）、プロセス管理２０１からの終了要求（ステップ１１０９）及び時間監視によるタイマ割り込みがある。

【００６６】ログ入力中断要求を受信した場合は（ステップ１１０５）、ログ入力を中断する（ステップ１１０６）。中断する要因は、正規化ログファイル４０の容量がＦＩＬＥ＿ＭＡＸＳＩＺＥ４７２に達したときである。

【００６７】ログ入力再開要求を受信した場合は（ステップ１１０７）、ログ入力を再開する（ステップ１１０８）。再開する要因は、正規化ログファイルをマネージャ１０へ転送したときである。

【００６８】終了要求を受信した場合は（ステップ１１０９）、ループを抜けて終了処理（ステップ１１１７）を行う。

【００６９】ログファイル監視ルール５００に設定された監視間隔に従ってログファイルの監視時刻になったとき、監視対象ログファイル群３０をオープンし（ステップ１１１１）、このログファイルのファイル管理情報を取得する。ファイル管理情報が前回取得したもの同じか否かを確認する（ステップ１１１２）。同じ場合は（ステップ１１１２ＹＥＳ）、前回オープンしたファイルと同じ内容であるため前回のファイルのオフセットからログデータを入力する（ステップ１１１３）。前回のファイルのオフセットは、当該ファイルについて前回入力済のレコードの次のレコードを指している。異なる場合は（ステップ１１１２ＮＯ）、新しいファイル（前回オープンしたファイルは削除された等）であると解釈し、先頭からログデータを入力する（ステップ１１１４）。その後、入力したログデータを正規化し（ステップ１１１５）、正規化ログデータをログファイル管理２０４へ通知する（ステップ１１１６）。ログデータの正規化は、上記のようにフォーマットルール５１０，５１５等を適用して行う。正規化ログデータをログファイル管理２０４に渡した後、当該ログファイルをクローズし、監視間隔に従って次の監視時刻にタイマを設定する。

【００７０】図２８は、エージェント２０のログファイル管理２０４の処理の流れを示すＰＡＤ図である。ログファイル管理２０４は、初期設定し（ステップ１２０１）、ルール管理２０３から動作条件ルール４７０とフィルタリングルール５２０を取得（ステップ１２０２）した後、プロセス管理２０１から終了要求が来るまでループし（ステップ１２０３）、イベントを待つ（ステップ１２０４）。イベントには、ログ入力２０２からの正規化ログデータ格納通知（ステップ１２０５）、マネージャ１０のログ収集１０７からのログ収集要求（ステップ１２０９）、ログファイル管理２０４自身からの正規化ログファイル容量確認要求（ステップ１２１１）、マネージャ１０のログ収集１０７からのマネージャ時刻の

16

通知（ステップ１２１６）と、プロセス管理２０１からの終了要求（ステップ１２１８）がある。

【００７１】正規化ログデータ格納通知を受信した場合は（ステップ１２０５）、ログ入力２０２から正規化ログデータを取得し（ステップ１２０６）、エージェントとマネージャの時間差（ステップ１２１７の処理結果）とログ出力時刻３２２から補正時刻３２３を計算する。ログ入力２０２から取得した正規化ログデータにこの補正時刻３２３を追加して正規化ログファイル４０に格納する（ステップ１２０７）。取得した正規化ログデータにフィルタリングルール５２０を適用して条件に合致する正規化ログデータのみを正規化ログファイル４０に格納する。次に正規化ログファイル容量確認要求を発行する（ステップ１２０８）。

【００７２】ログ収集要求を受信した場合は（ステップ１２０９）、正規化ログファイル４０中の正規化ログデータを補正時刻３２３の順にソートした後、ＭＡＮＡＧＥＲ＿ＡＤＤＲＥＳＳ４７１に示されるマネージャ１０へ転送する（ステップ１２１０）。

【００７３】正規化ログファイル容量確認要求を受信した場合は（ステップ１２１１）、正規化ログファイルの使用容量とＦＩＬＥ＿ＭＡＸＳＩＺＥ４７２を比較し（ステップ１２１２）、最大サイズに達したとき（ステップ１２１２ＹＥＳ）は、ログ入力２０２へ中断通知を発行する（ステップ１２１３）。最大サイズに達していないとき（ステップ１２１２ＮＯ）は、前回中断要求を発行したか確認し（ステップ１２１４）、発行していたとき（ステップ１２１４ＹＥＳ）は、ログ入力２０２へログ入力再開要求を通知する（ステップ１２１５）。

【００７４】マネージャ時刻の通知を受信した場合は（ステップ１２１６）、エージェントとマネージャのコンピュータ時刻の差を計算する（ステップ１２１７）。

【００７５】終了要求を受信した場合は（ステップ１２１８）、ループを抜けて終了処理（ステップ１２１９）を行う。

【００７６】

【発明の効果】以上説明したように本発明によれば、エージェントが複数のログファイルを監視し種々の形式で出力されたログデータを入力した後、正規化を行い共通的なデータ形式に変換する。また必要なログデータだけを抽出し、ログデータの出力時刻としてマネージャの時計に合わせた補正時刻を使用するようにしたので、運用者はネットワークに存在する複数のコンピュータのログデータを統一したデータ形式及び時刻に基づいて解析することができる。

【００７７】またマネージャが蓄積するログデータについては、所定期間のログデータを保存するようにしたので、古いログデータから順に削除する形でログ情報の維持を規制できる。

【００７８】さらに収集したログデータを補正時刻及び

正規化項目によって検索可能としたので、運用者は必要なログ情報を容易に取得できる。

【図面の簡単な説明】

【図１】実施形態のネットワークシステムの構成図である。

【図２】実施形態のマネージャとエージェントが行う処理動作の概略を示す図である。

【図３】実施形態のマネージャ１０の構成を示す機能ブロック図である。

【図４】実施形態のエージェント２０の構成を示す機能ブロック図である。

【図５】実施形態の正規化ログデータの概略構成を示す図である。

【図６】実施形態の共通情報クラスのデータ構成を示す図である。

【図７】実施形態のユーザ情報クラスのデータ構成を示す図である。

【図８】実施形態のサービス情報クラスのデータ構成を示す図である。

【図９】実施形態のアドレス情報クラスのデータ構成を示す図である。

【図１０】実施形態のファイル情報クラスのデータ構成を示す図である。

【図１１】実施形態のトラフィフィック情報クラスのデータ構成を示す図である。

【図１２】実施形態の個別情報クラスのデータ構成を示す図である。

【図１３】実施形態のデータ格納クラスのデータ構造を示す図である。

【図１４】正規化項目のコード化テーブルの例を示す図である。

【図１５】マネージャルールの例を示す図である。

【図１６】エージェントの動作条件ルールの例を示す図である。

【図１７】エージェントのログファイル監視ルールの例を示す図である。

【図１８】エージェントのフォーマットルール（その１）の例を示す図である。

【図１９】エージェントのフォーマットルール（その２）の例を示す図である。

【図２０】エージェントのフィルタリングルールの例を示す図である。

【図２１】監視対象ログファイルのログデータであるメッセージテキストの例を示す図である。

【図２２】実施形態の正規化ログデータベースのデータ構造を示す図である。

【図２３】実施形態のマネージャが行うルール配布の処理の流れを示すＰＡＤ図である。

【図２４】実施形態のマネージャが行うログ収集の処理の流れを示すＰＡＤ図である。

【図２５】実施形態のマネージャが行う構成管理の処理の流れを示すＰＡＤ図である。

【図２６】実施形態のマネージャが行うデータベース管理の処理の流れを示すＰＡＤ図である。

【図２７】実施形態のエージェントが行うログ入力の処理の流れを示すＰＡＤ図である。

【図２８】実施形態のエージェントが行うログファイル管理の処理の流れを示すＰＡＤ図である。

【符号の説明】

１０・・・マネージャ、２０・・・エージェント、４０・・・正規化ログファイル、５０・・・正規化ログデータベース、８０・・・ネットワーク管理システム、１０４・・・構成管理、１０６・・・ルール配布、１０７・・・ログ収集、１０９・・・データベース管理、１１０・・・ルール、２０２・・・ログ入力、２０４・・・ログファイル管理、２０５・・・ルール

【図７】

図７

ユーザ情報クラス	～３０２
ユーザ名	～３３０
ＵＩＤ	～３３１
変更後のユーザ名	～３３２
変更後のＵＩＤ	～３３３
セキュリティレベル	～３３４
アクセス機	～３３５
アクセス結果	～３３６
端末名	～３３７

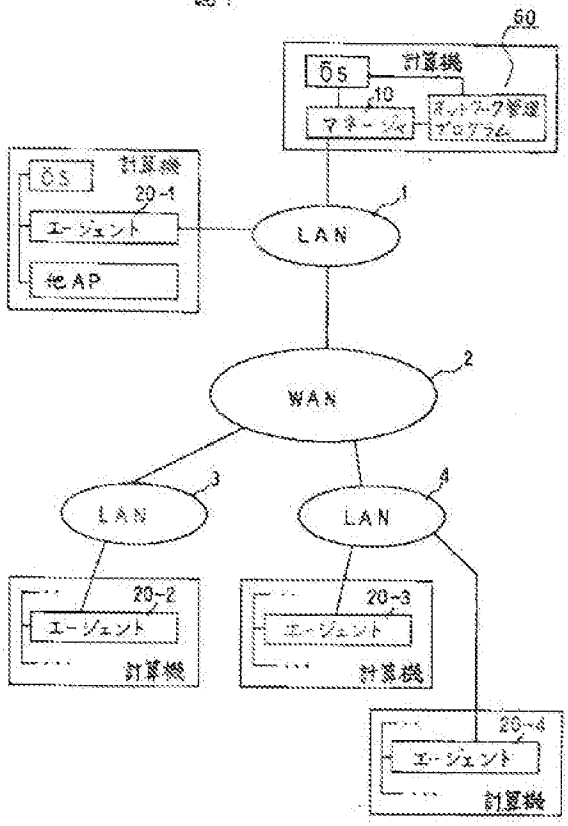
【図８】

図８

サービス情報クラス	～３０３
サービス名	～３４０
サービスバージョン	～３４１
プロセス名	～３４２
プロセスＩＤ	～３４３

【図1】

図1



【図5】

図5

正規化ログデータ　～300	
共通情報クラス	～301
ユーザ情報クラス	～302
サービス情報クラス	～303
アドレス情報クラス	～304
ファイル情報クラス	～305
・ ・ ・	
トラフィック情報クラス	～306
個別情報クラス	～307

【図6】

図6

共通情報クラス　～301		
正規化バージョン		～310
ログ種別	ログ事象	～311
	ログ事象結果	～312
	ログ出力プログラム	～313
	データ格納クラス	～314
	ログファイル名	～315
マネージャ	ホスト名	～316
	ホストIPアドレス	～317
エージェント	ホスト名	～318
	ホストIPアドレス	～319
監視対象	ホスト名	～320
	ホストIPアドレス	～321
時刻	ログ出力時刻	～322
	補正時刻	～323
フィルタリングルール名		～324

【図11】

図11

トラフィック情報クラス　～306
受信バイト数
送信バイト数
処理時間

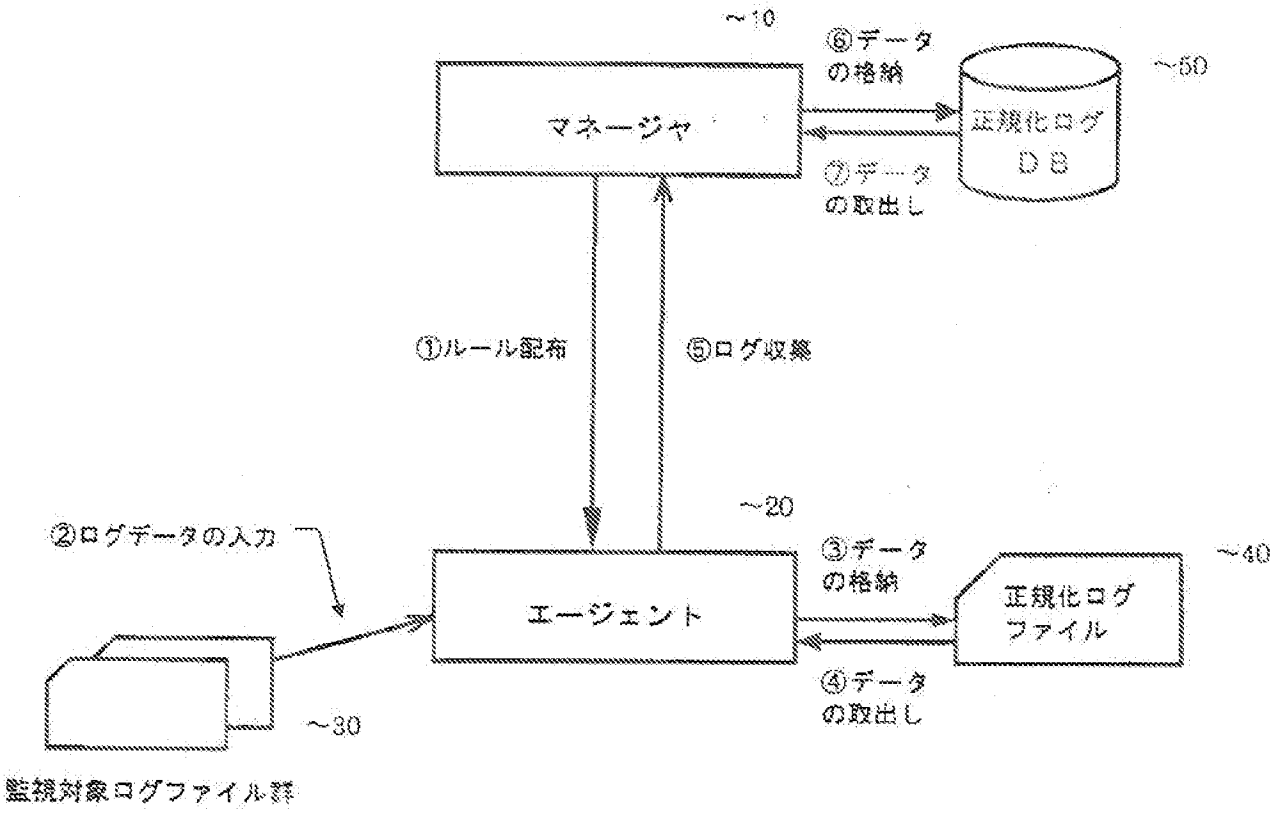
【図12】

図12

個別情報クラス　～307
メッセージテキスト

【図2】

図2



【図9】

図9

アドレス情報クラス　～304

接続元ホスト名	～350
接続元ＩＰアドレス	～351
接続元ＭＡＣアドレス	～352
接続元ポート番号	～353
接続先ホスト名	～354
接続先ＩＰアドレス	～355
接続先ＭＡＣアドレス	～356
接続先ポート番号	～357
コネクション状態	～358
開始時刻	～359
終了時刻	～360
アクセス結果	～361

【図15】

図15

マネージャルール　～450

DB_MAX：正規化ログデータの保存期間； ～451
RULE_MAX：ルール配布の最大多重度； ～452
LOG_MAX：ログ収集の最大多重度； ～453

【図16】

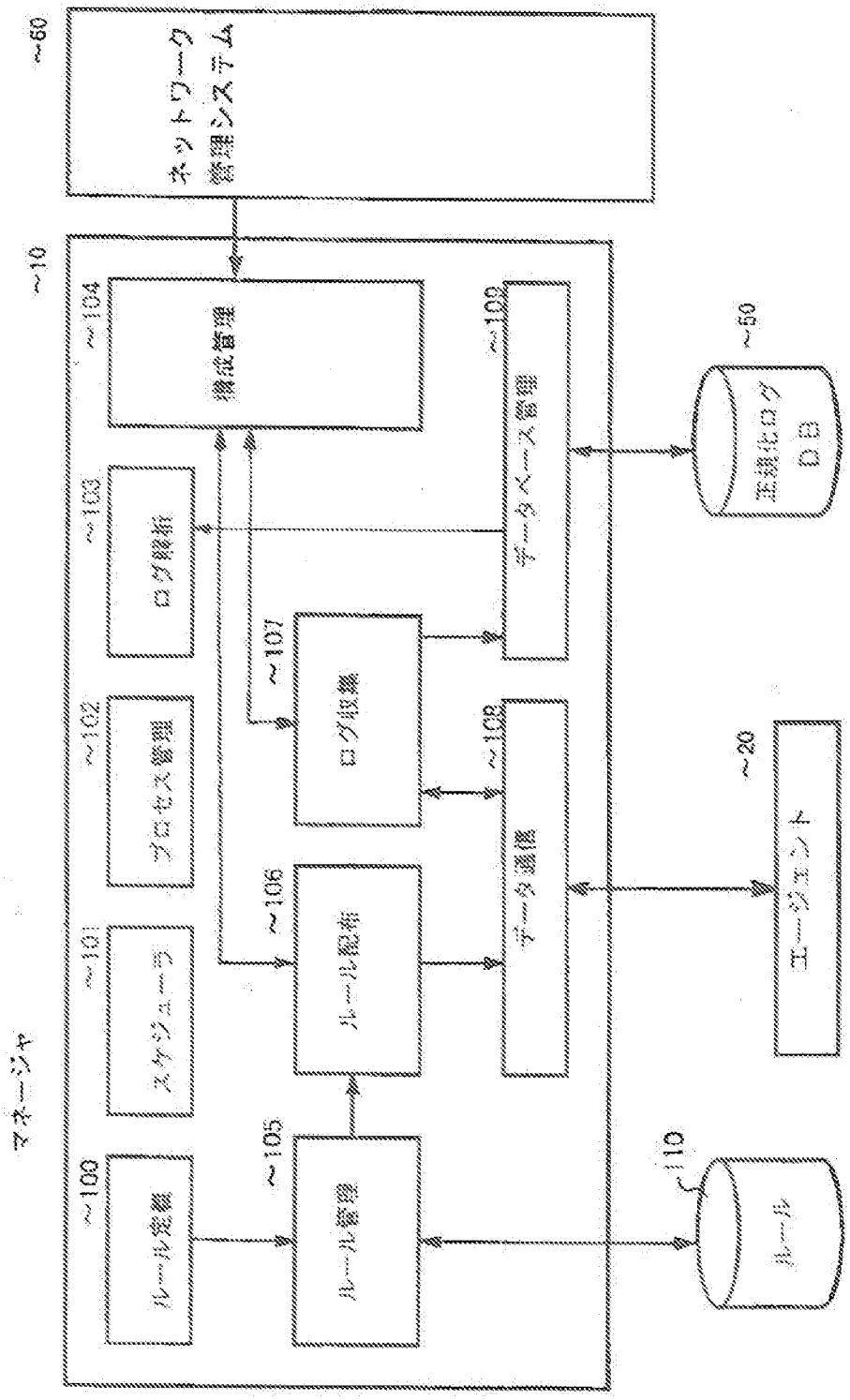
図16

動作条件ルール　～470

MANAGER_ADDRESS：マネージャのＩＰアドレス； ～471
FILE_MAXSIZE：正規化ファイルの最大サイズ； ～472

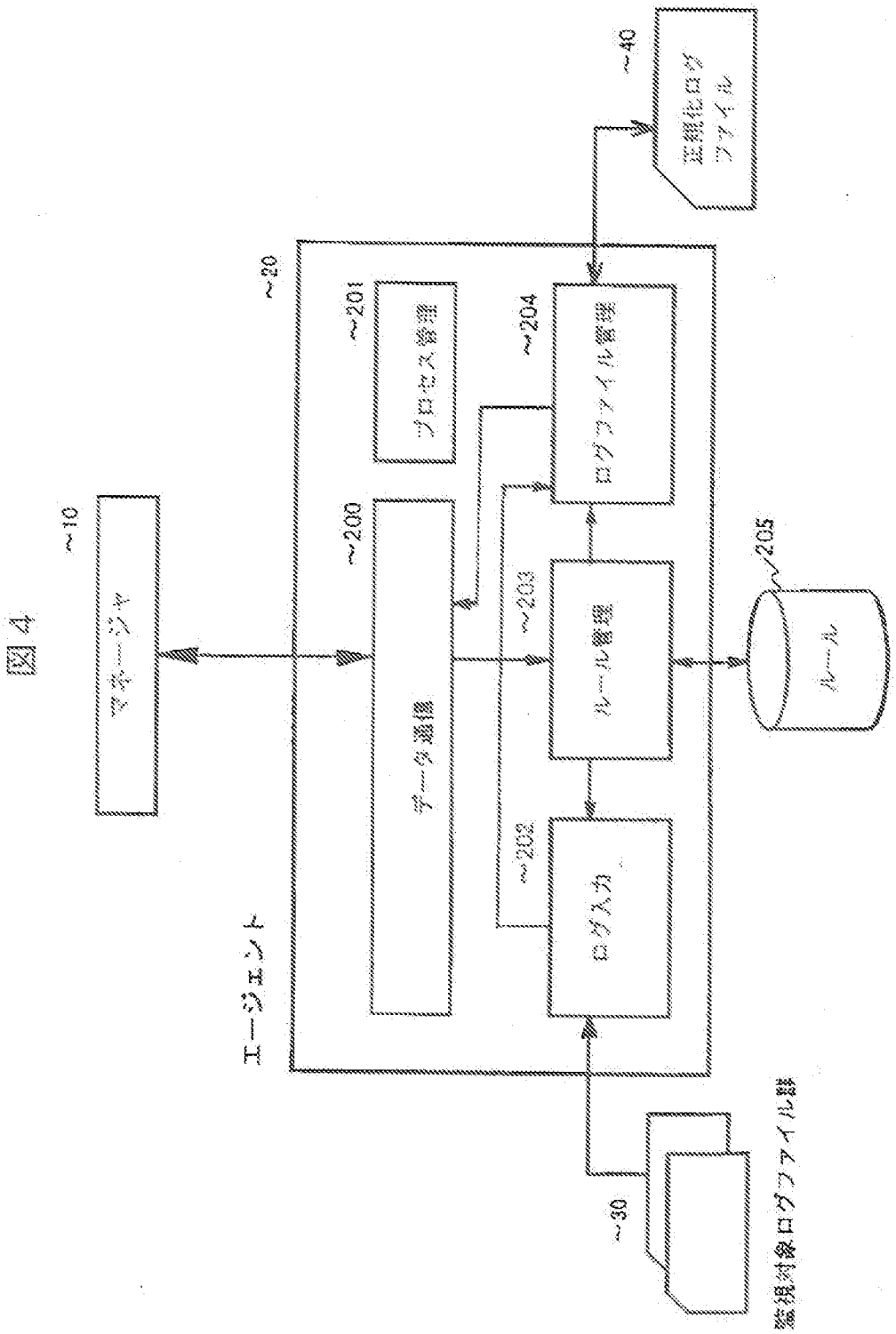
【図3】

図3


マネージャ
~60
ネットワーク管理システム
~10
~104
構成管理
~103
ログ解析
~102
プロセス管理
~101
スケジューラ
~100
ルール定義
~105
ルール管理
~106
ルール起動
~107
ログ収集
~108
データ通信
~102
データベース管理
~50
正規化ログDB
~20
エージェント
~110
ルール

【図4】

図4


~10
マネージャ
~20
エージェント
~200
データ通信
~201
プロセス管理
~202
ログ入力
~203
ルール管理
~204
ログファイル管理
~205
ルール
~30
監視対象ログファイル群
~40
正規化ログファイル

【図１０】

図１０

ファイル情報クラス　～305

ファイル名	
変更後	作成時刻
	最終修正時刻
	最終アクセス時刻
	ｉ－ｎｏｄｅ番号
	アクセス許可
	ＵＩＤ
	ＧＩＤ
	サイズ
変更前	作成時刻
	最終修正時刻
	最終アクセス時刻
	ｉ－ｎｏｄｅ番号
	アクセス許可
	ＵＩＤ
	ＧＩＤ
	サイズ

【図１３】

図１３

データ格納クラス　～314

Ｔ１	Ｌ１	Ｖ１（存在する情報クラスの指定領域）						
		Ｔ２	Ｌ２	Ｖ２	Ｔ５	Ｌ５	Ｖ５	……

【図１８】

図１８

フォーマットルール（その１）　～510

```
FMT_1 : REGTEXT == "文字列１" | ログ収集 == "y" | ログ収集結果 == "n" :
正規化項目１(文字数)：正規化項目２(終了文字)：…；
FMT_1 : REGTEXT == "文字列２" && REGTEXT == "文字列３" | ログ収集 == "y"
| ログ収集結果 == "f" : 正規化項目１(終了文字)：SKIP(読み飛ばし文字数)：
正規化項目４(文字数)：…；
```

【図１９】

図１９

フォーマットルール（その２）　～515

```
FMT_2 :  REGTEXT == "文字列５" && REGTEXT == "文字列６" | ログ収集 == "z"
| ログ収集結果 == "t" : 正規化項目１(終了文字)：SKIP("区切り文字")：正規
化項目３(文字数)：…；
```

【図１７】

図１７

ログファイル監視ルール　～500

```
TARGET_LOG : "監視対象ログファイル名１", FORMAT=SEQ, INTERVAL=時間,
FMT_NAME="フォーマットルール名" ;
TARGET_LOG : "監視対象ログファイル名２", FORMAT=WRAP, INTERVAL=時間 ;
```

【図２１】

図２１

メッセージテキスト例　～550

```
SU 01/30 11:18 + ttyp5 fujimo-root                                    ～551
SU 01/31 11:52 - ttyp7 morita-sbc                                     ～552

Jan  4 12:38:10 hosta ftpd[1111]: connect from 170.213.252.12         ～553
Jan 12 13:12:15 hosta ftpd[1111]: refused connect from hostb          ～554
Jan 18 15:10:55 hosta ftpd[2222]: connect to hosta                    ～555

Jan 25 10:12:34 hosta job[2222]: ジョブA80を開始しました。            ～556
Jan 25 10:15:10 hosta job[2222]: ジョブA80が異常終了しました。        ～557
```

【図２０】

図２０

フィルタリングルール　～520

```
FLT : 正規化項目１ == "文字列１" ;
FLT : 正規化項目２ == "文字列２" || 正規化項目３ == "文字列３" ;
FLT : 正規化項目４ == "文字列４" && 正規化項目５ != "文字列５" ;
FLT : 正規化項目６ == "時刻1" ～"時刻2" && 正規化項目７ == "文字列７" ;
```

【図14】

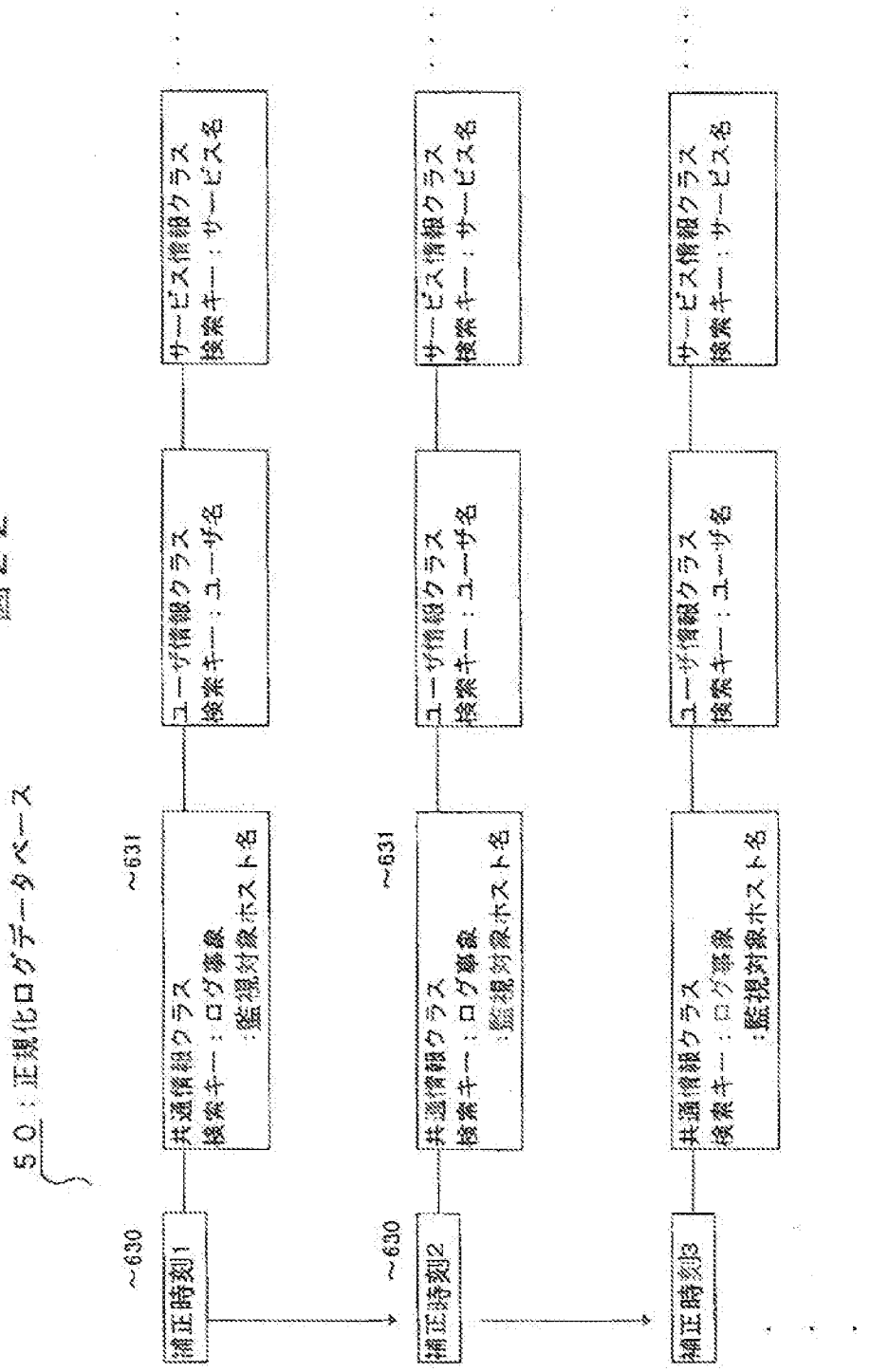
図14

正規化項目のコード化テーブル ～600

正規化項目	内容	コード
ログ事象	login	1
	su（ユーザ変更）	2
	connect	3
	ファイル	4
	ジョブ	5
	メール	6
ログ事象結果	成功	0
	失敗	1
アクセス権	あり	0
	なし	1
アクセス結果	成功	0
	失敗	1
アクセス許可	あり	0
	なし	1

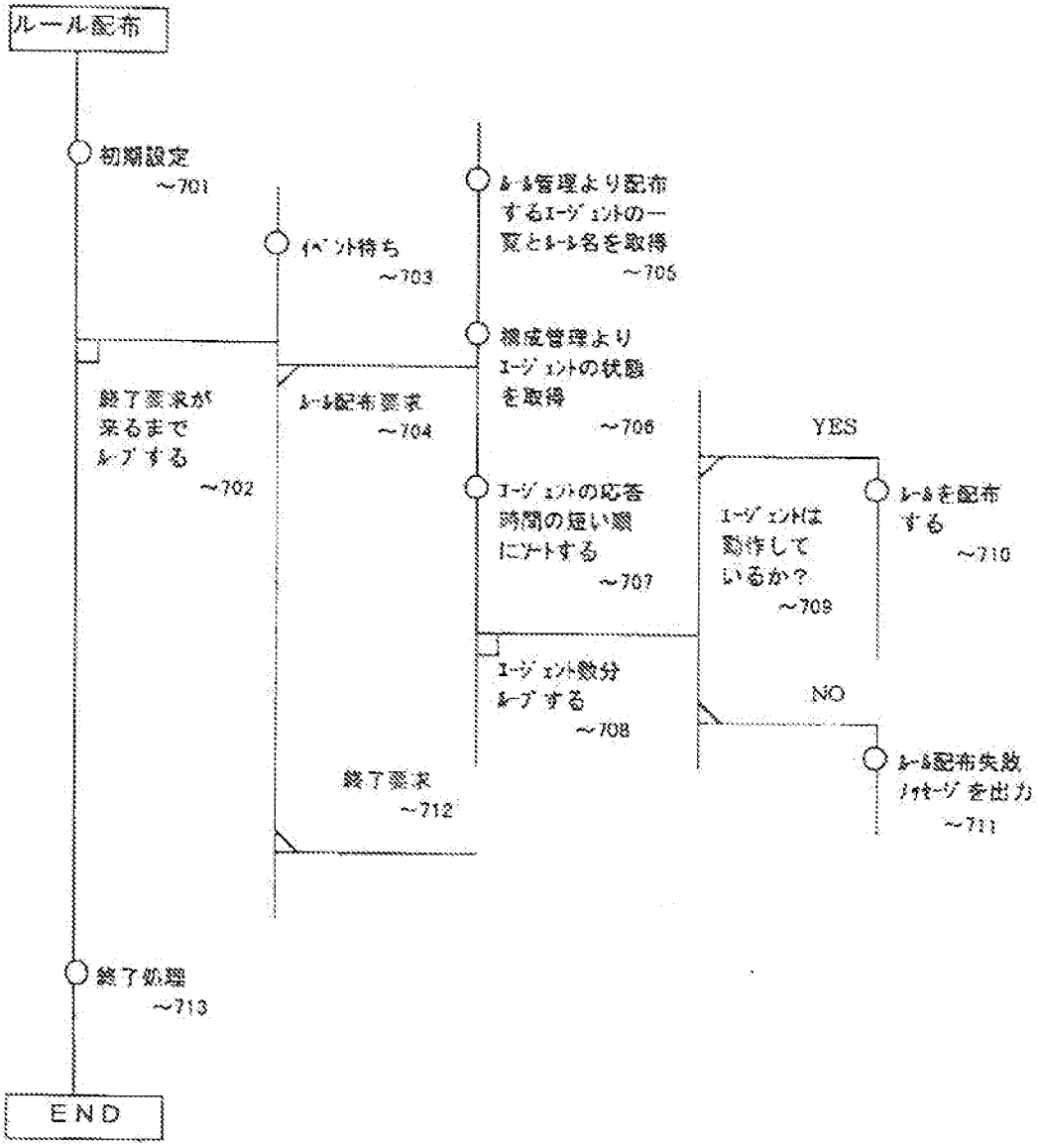
【図22】

図22


50：正規化ログデータベース
～630
～631
補正時刻1
補正時刻2
補正時刻3
共通情報クラス
検索キー：ログ事象
：監視対象ホスト名
ユーザ情報クラス
検索キー：ユーザ名
サービス情報クラス
検索キー：サービス名

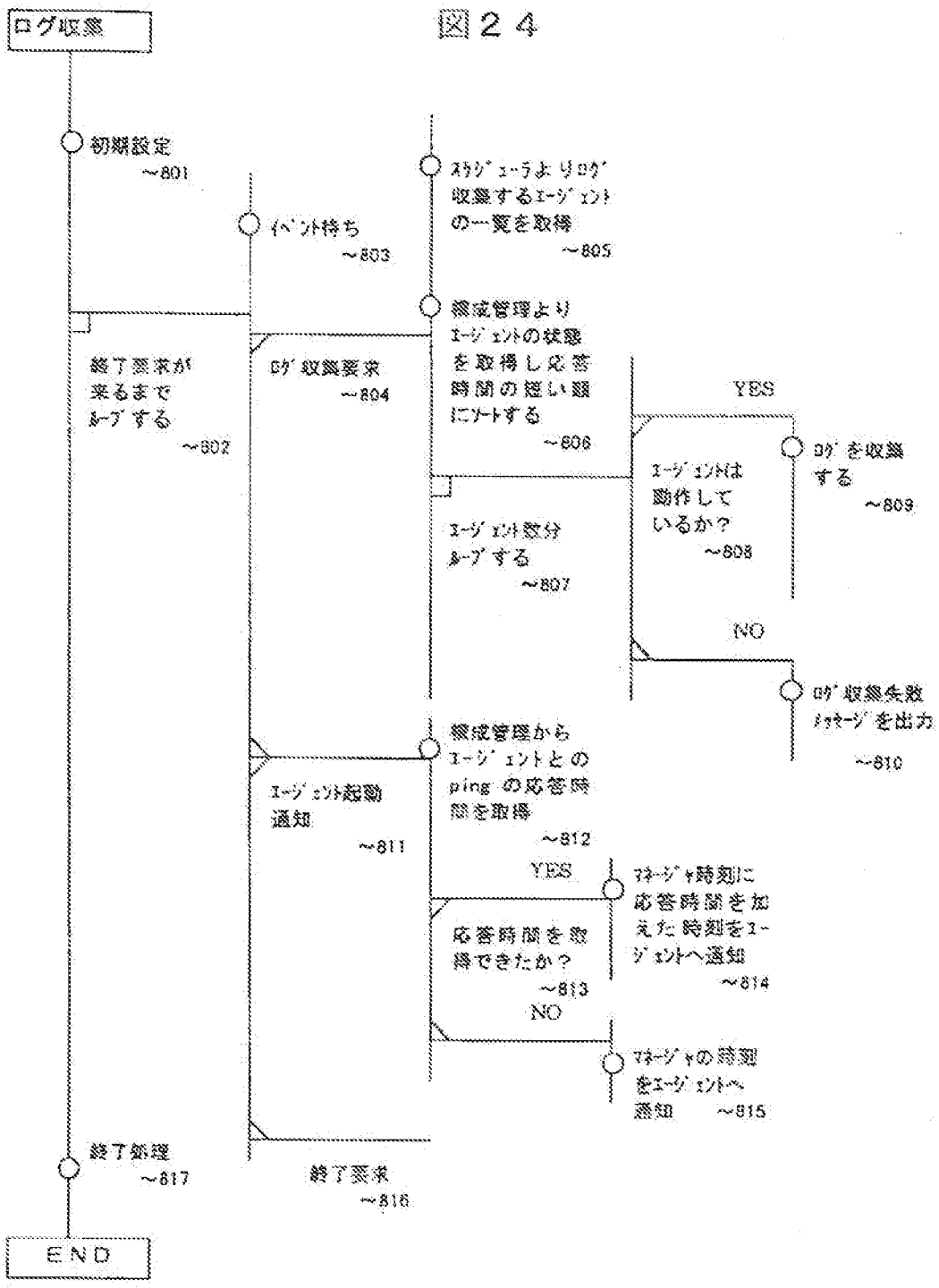
【図23】

図23


ルール配布
初期設定
～701
イベント待ち
～703
ルール管理より配布するエージェントの一覧とルール名を取得
～705
構成管理よりエージェントの状態を取得
～706
終了要求が来るまでループする
～702
ルール配布要求
～704
エージェントの応答時間の短い順にソートする
～707
YES
エージェントは動作しているか？
～709
ルールを配布する
～710
エージェント数分ループする
～708
NO
ルール配布失敗メッセージを出力
～711
終了要求
～712
終了処理
～713
END

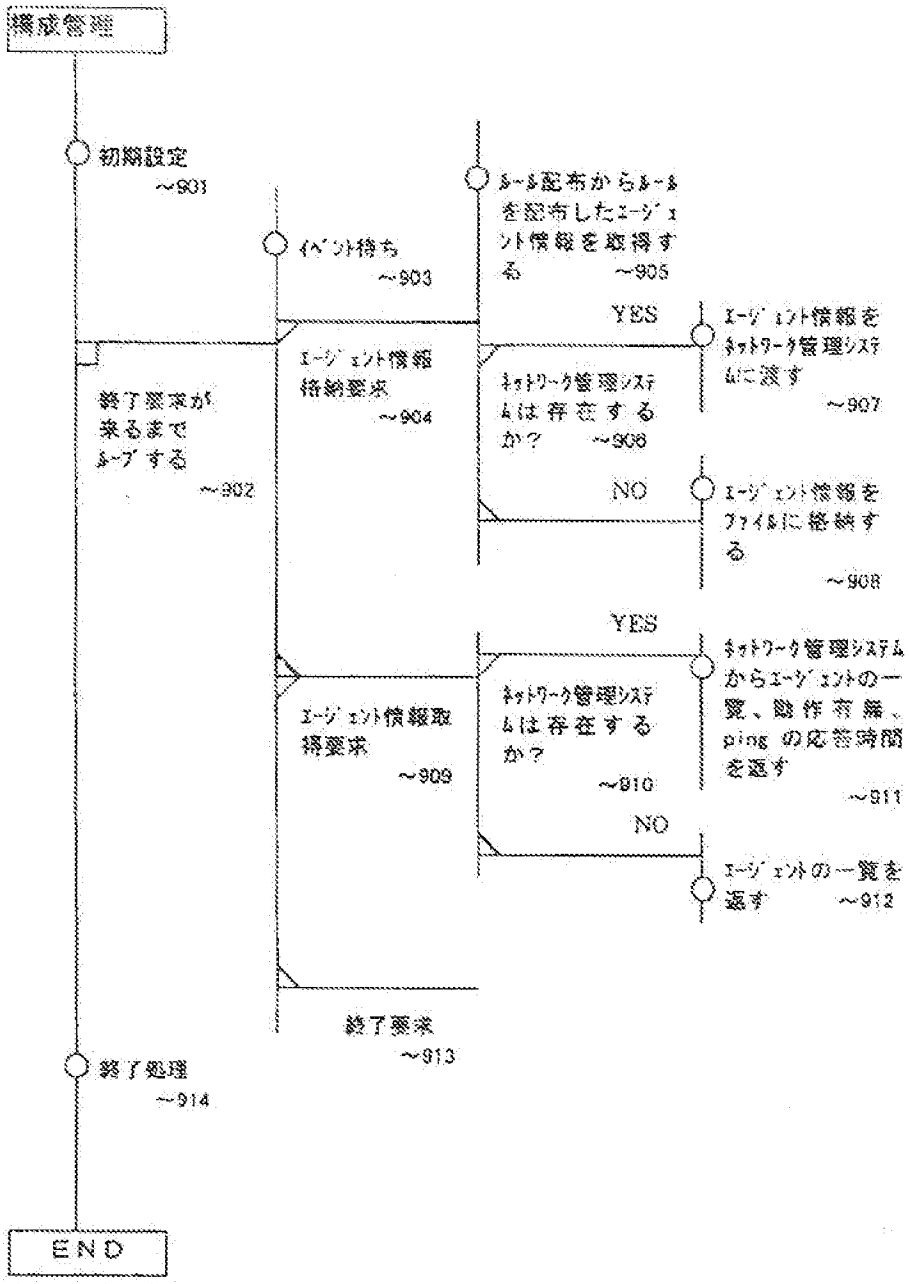
【図24】

図24


ログ収集
初期設定
~801
イベント待ち
~803
スケジューラよりログ収集するエージェントの一覧を取得
~805
構成管理よりエージェントの状態を取得し応答時間の短い順にソートする
~806
終了要求が来るまでループする
~802
ログ収集要求
~804
YES
エージェントは動作しているか？
~808
ログを収集する
~809
エージェント数分ループする
~807
NO
ログ収集失敗メッセージを出力
~810
構成管理からエージェントとのpingの応答時間を取得
~812
エージェント起動通知
~811
YES
マネージャ時刻に応答時間を加えた時刻をエージェントへ通知
~814
応答時間を取得できたか？
~813
NO
マネージャの時刻をエージェントへ通知
~815
終了処理
~817
終了要求
~816
END

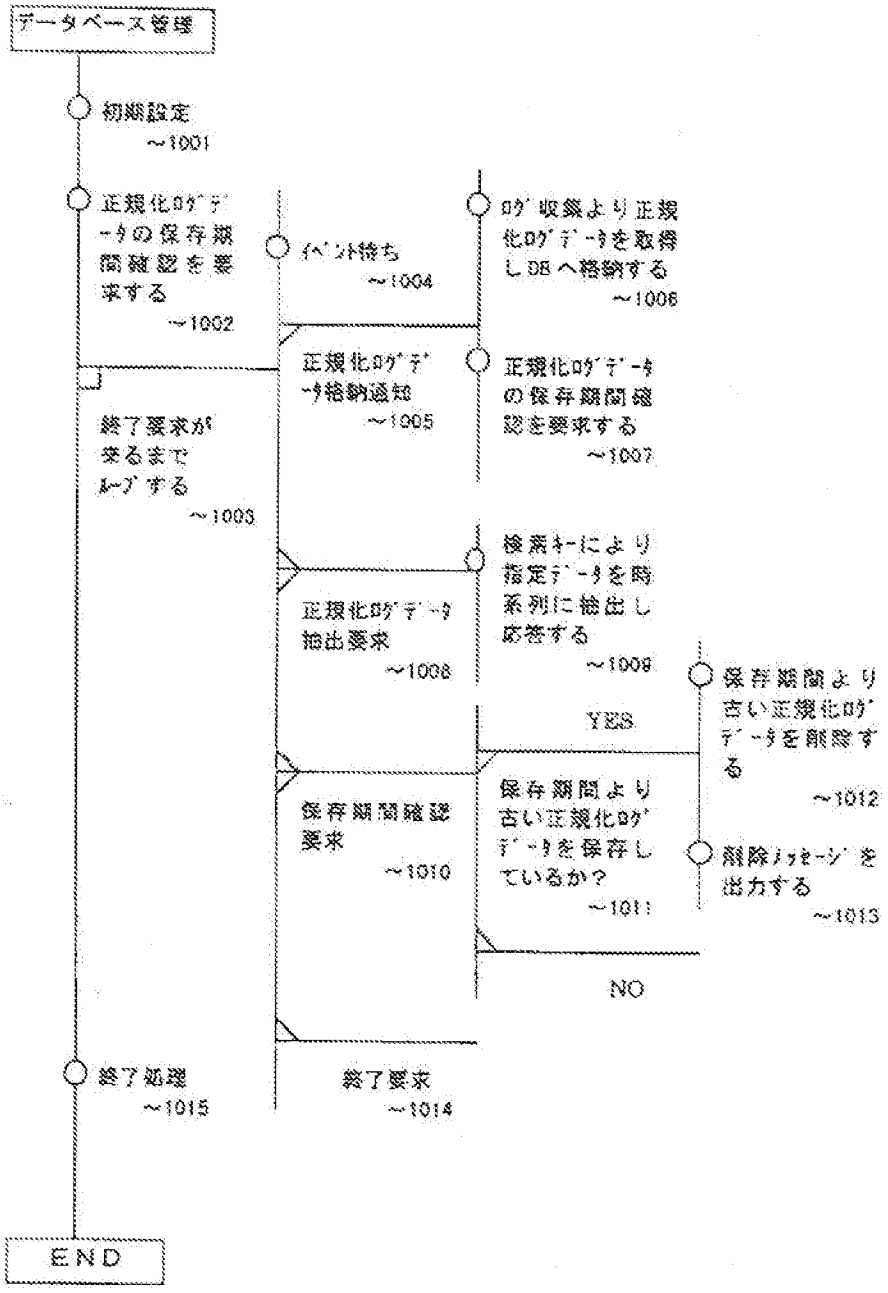
【図25】

図25


構成管理
初期設定
～901
イベント待ち
～903
ルール配布からルールを配布したエージェント情報を取得する
～905
YES
エージェント情報をネットワーク管理システムに渡す
～907
ネットワーク管理システムは存在するか？
～906
NO
エージェント情報をファイルに格納する
～908
エージェント情報格納要求
～904
終了要求が来るまでループする
～902
YES
ネットワーク管理システムからエージェントの一覧、動作有無、ping の応答時間を返す
～911
ネットワーク管理システムは存在するか？
～910
NO
エージェントの一覧を返す
～912
エージェント情報取得要求
～909
終了要求
～913
終了処理
～914
END

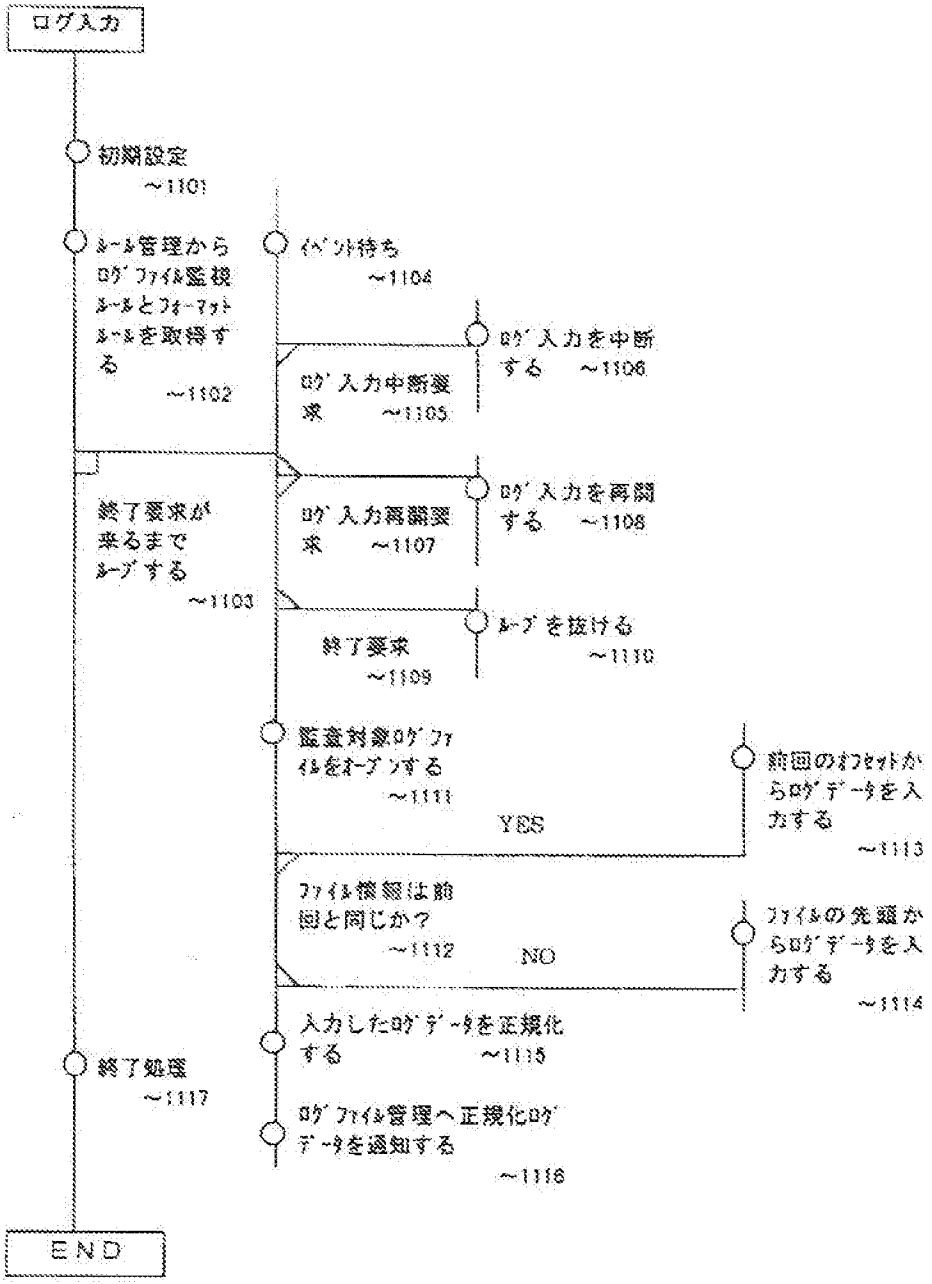
【図26】

図26


データベース管理
初期設定
~1001
正規化ログデータの保存期間確認を要求する
~1002
終了要求が来るまでループする
~1003
イベント待ち
~1004
正規化ログデータ格納通知
~1005
ログ収集より正規化ログデータを取得しDBへ格納する
~1006
正規化ログデータの保存期間確認を要求する
~1007
検索キーにより指定データを時系列に抽出し応答する
~1009
正規化ログデータ抽出要求
~1008
YES
保存期間より古い正規化ログデータを削除する
~1012
保存期間確認要求
~1010
保存期間より古い正規化ログデータを保存しているか?
~1011
削除メッセージを出力する
~1013
NO
終了処理
~1015
終了要求
~1014
END

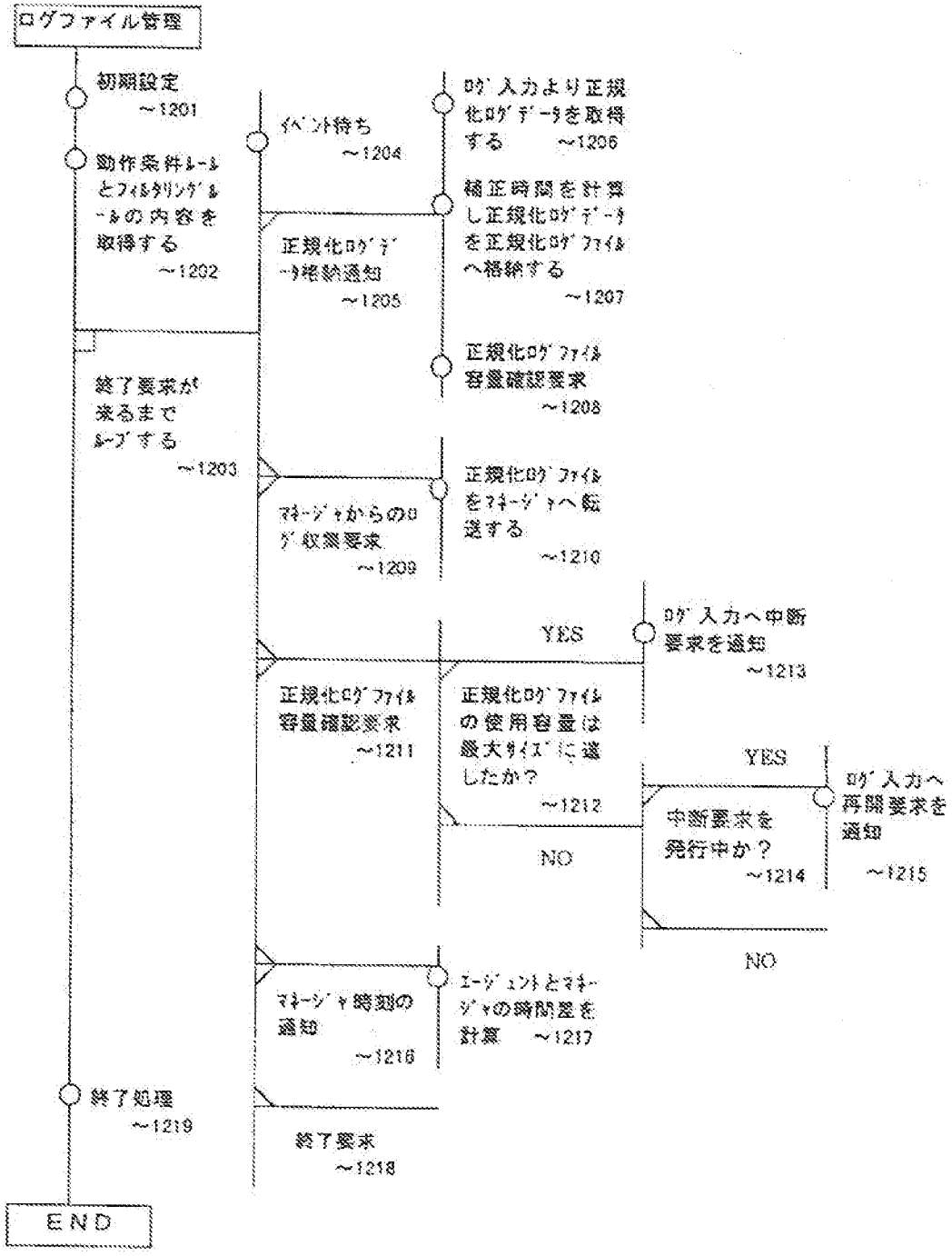
【図２７】

図２７


ログ入力
初期設定
～1101
ルール管理からログファイル監視ルールとフォーマットルールを取得する
～1102
イベント待ち
～1104
ログ入力中断要求
～1105
ログ入力を中断する
～1106
ログ入力再開要求
～1107
ログ入力を再開する
～1108
終了要求
～1109
ループを抜ける
～1110
終了要求が来るまでループする
～1103
監査対象ログファイルをオープンする
～1111
YES
前回のオフセットからログデータを入力する
～1113
ファイル情報は前回と同じか？
～1112
NO
ファイルの先頭からログデータを入力する
～1114
入力したログデータを正規化する
～1115
ログファイル管理へ正規化ログデータを通知する
～1116
終了処理
～1117
END

【図２８】

図２８



フロントページの続き

(72)発明者　中野　秀紀
東京都千代田区大手町二丁目６番２号　株式会社日立情報ネットワーク内

(72)発明者　森田　眞司
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　山田　賞
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　新村　美貴
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

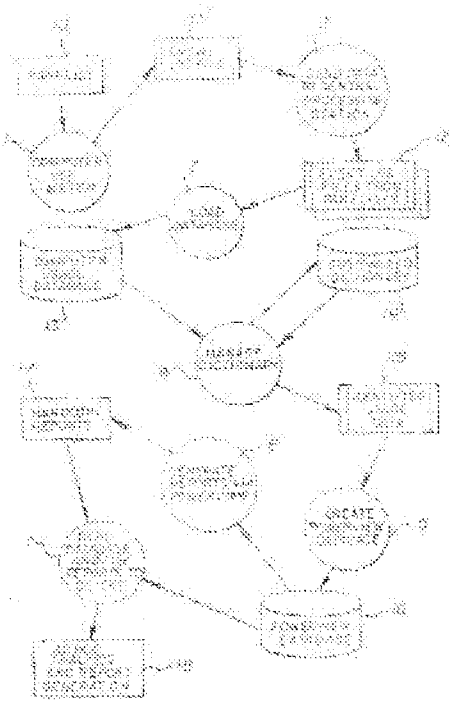
Computer use meter and analyzer

Publication number: JP10510647 (T)
Publication date: 1998-10-13
Inventor(s):
Applicant(s):
Classification:
- International: ***G06F1/00; G05F11/34; G06F13/00; G06F15/00; G06F21/00; H04Q9/00;*** (IPC1-7): G06F11/34; G06F13/00; H04Q9/00
- European: G06F11/34T; G06F21/00N3J1; G06Q30/00A
Application number: JP19960502197T 19960607
Priority number(s): WO1996US10091 19960607; US19950474082 19950607

Also published as:
US6115680 (A)
US5675510 (A)
WO9641495 (A1)
NO975728 (A)
MX9709752 (A)
more >>

Abstract not available for JP 10510647 (T)
Abstract of corresponding document: **US 6115680 (A)**

PCT No. PCT/US96/10091 Sec. 371 Date Mar. 2, 1998 Sec. 102(e) Date Mar. 2, 1998 PCT Filed Jun. 7, 1996 PCT Pub. No. WO96/41495 PCT Pub. Date Dec. 19, 1996The subject system measures and reports the use of a personal computer by a user through a log file. The log file includes entries corresponding to predetermined events and can report on the applications used and communication functions engaged in by the user. The log files from one or more computers may be assembled and analyzed in order to ascertain computer use habits for computer software, computer hardware and computer communications. The system may also be used to predict computer use trends and to represent computer use history.



(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号

特表平10－510647

(43)公表日　平成10年(1998)10月13日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	11/34		Ｇ０６Ｆ	11/34	Ｃ
	13/00	３５４		13/00	３５４Ｄ
Ｈ０４Ｑ	9/00	３０１	Ｈ０４Ｑ	9/00	３０１Ｂ
		３１１			３１１Ｈ

審査請求　有　　予備審査請求　有　（全 30 頁）

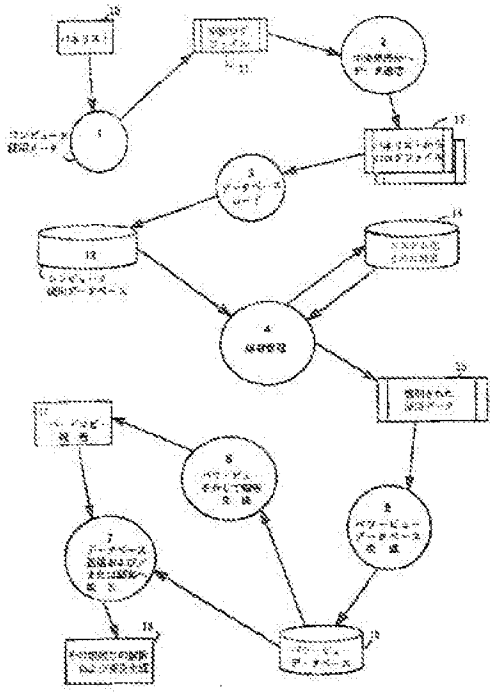
(21)出願番号　特願平9－502197
(86)(22)出願日　平成８年(1996)６月７日
(85)翻訳文提出日　平成９年(1997)12月８日
(86)国際出願番号　ＰＣＴ／ＵＳ９６／１００９１
(87)国際公開番号　ＷＯ９６／４１４９５
(87)国際公開日　平成８年(1996)12月19日
(31)優先権主張番号　０８／４７４，０８２
(32)優先日　1995年６月７日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　メディア・メトリックス・インコーポレーテッド
アメリカ合衆国、　ニューヨーク州　11050、ポート・ワシントン、ウエスト・ショアー・ロード　900
(72)発明者　コフィー、　スティーブン・アール
アメリカ合衆国、　ニューヨーク州　11937、イースト・ハンプトン、スプリングス・フィアープレイス・ロード　487
(74)代理人　弁理士　鈴江　武彦　（外４名）

最終頁に続く

(54)【発明の名称】　コンピュータ使用メーターおよび解析装置

(57)【要約】
本発明のシステムは、ログファイル(11)を通してユーザーによるパーソナルコンピュータの使用量を測定して報告する。ログファイル(11)は、予め定められた事象に対応した項目を含み、使用されたアプリケーション、およびユーザーがたずさわった通信機能において報告することができる。１以上のコンピュータからのログファイル(11)は、コンピュータソフトウェア、コンピュータハードウェア、およびコンピュータ通信に対するコンピュータ使用の性質を確認するために収集され、解析されてもよい。システムはまた、コンピュータ使用傾向を予測し、またコンピュータ使用ヒストリィを表すために使用されてもよい。



Ｆｉｇｕｒｅ１

【特許請求の範囲】

1．ユーザー・コンピュータ・マシン中に設置され、前記コンピュータ・マシンのメモリに記憶された予め定められたマシン動作事象のログをそれぞれ含んでいる複数のローカル・コンピュータ使用メーターと、

コンピュータ・マシン中に設置され、予め定められたマシン動作事象のログをコンピュータ・メモリにロードする処理ステーションと、

コンピュータ・マシン中に設置され、前記コンピュータ・マシンのメモリに記憶されたマシン動作事象に基づいてアクセス、処理および報告の作成をするように構成されたデータベース管理システムとを含んでおり、

前記処理ステーションが、前記複数のローカル・コンピュータ使用メーターにリンクされているコンピュータ使用監視システム。

2．前記処理ステーションは、電子通信チャンネルによって前記複数のローカル・コンピュータ使用メーターにリンクされている請求項1記載のコンピュータ使用監視システム。

3．前記電子通信チャンネルは、予め定められた基準に基づいて設定されている請求項2記載のコンピュータ使用監視システム。

4．前記予め定められた基準は周期的である請求項3記載のコンピュータ使用監視システム。

5．前記予め定められた基準は、前記ログによって占有されたメモリの量に基づいている請求項3記載のコンピュータ使用監視システム。

6．前記処理ステーションは、ユーザーコンピュータマシンから可搬性媒体に記録を転送する手段と、可搬性媒体から処理ステーションに前記記録を転送する手段とによって前記複数のローカル・コンピュータ使用メーターにリンクされる請求項1記載のコンピュータ使用監視システム。

7．前記予め定められたマシン動作事象は、オペレーティングシステムのコール・バック・メッセージに対応した事象を含んでいる請求項1記載のコンピュータ使用監視システム。

8．前記予め定められたマシン動作事象は、受取られたモデム文字ストリングに対応した事象を含んでいる請求項1記載のコンピュータ使用監視システム。

９．さらに、前記処理ステーションと関連したコンピュータメモリに記憶された辞書ファイルと、

ログファイルに書込まれたマシン動作事象を辞書ファイルを参照することによって解釈する手段とを含んでいる請求項１記載のコンピュータ使用監視システム。

１０．オペレーティングシステム・メッセージを傍受して、オペレーティングシステム・メッセージモジュールに応答する予め定められたタイプのメッセージの受信を示し、

選択されたオペレーティングシステム・メッセージに応答する事象ログを作成および記憶し、

１以上のコンピュータシステムから中央システムに１以上の事象ログを転送し、

前記事象ログの内容を解析するステップを含んでいるコンピュータの使用監視方法。

１１．複数の各ユーザー使用コンピュータシステムにおいて多数のマシン動作事象を生成し、

前記ユーザーコンピュータシステムのローカル・コンピュータメモリ中のログに各事象を記憶し、

前記ユーザーコンピュータシステムから処理ステーションコンピュータに前記記憶された事象を転送し、

前記処理ステーションコンピュータと関連したメモリに前記事象ログをロードし、

前記処理ステーションコンピュータと関連したメモリに記憶された辞書を参照することによって前記事象ログを解釈し、

前記解釈されたコンピュータ事象ログを特定の基準にしたがって編集および報告するステップを含んでいる複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

１２．前記転送するステップは、電子通信チャンネルを介して行われる請求項１１記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定

する方法。

１３．前記転送するステップは、予め定められた基準に基づいて開始される請求項１２記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

１４．前記予め定められた基準は、周期的である請求項１３記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

１５．前記予め定められた基準は、前記ログによって占有されたメモリの量に基づいている請求項１３記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

１６．前記転送するステップは、ユーザーコンピュータマシンから可搬性磁気媒体に記録を転送して、前記可搬性磁気媒体から前記処理ステーションコンピュータに前記記録を転送する請求項１１記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

１７．前記マシン動作事象は、オペレーティングシステム・コールバック・メッセージに対応した予め定められた事象を含んでいる請求項１１記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

１８．前記マシン動作事象は、傍受されたモデム文字ストリングに対応した事象を含んでいる請求項１１記載の複数のコンピュータ・システムによってコンピュータ使用の性質を決定する方法。

１９．コンピュータモニタ上に表示された情報を周期的に監査し、

使用活動を示すラベルのログを作成および記憶するステップを含んでいるコンピュータ使用監視方法。

２０．前記監査するステップは、予め選択されたコンピュータ・アプリケーション・プログラムによって表示された情報をポーリングでチェックする請求項１９記載のコンピュータ使用監視方法。

２１．前記予め選択されたコンピュータアプリケーション・プログラムは、オン・ラインサービス・アクセスおよびインターフェイス・プログラムであり、前記ラベルのログを作成および記憶するステップは、活動的な表示要素タイトルをロ

グファイルに書込む請求項２０記載のコンピュータ使用監視方法。

２２．前記監査するステップは、表示要素の内容を監視して、予め定められた基準を満足させる表示要素内容を識別し、

前記作成および記憶するステップは、識別された表示要素の内容をログファイルに書込む請求項１９記載のコンピュータ使用監視方法。

２３．前記表示要素は編集ボックスであり、前記予め定められた基準は予め定められたシンタクスである請求項２２記載のコンピュータ使用メーター。

２４．前記シンタクスは、ＵＲＬシンタクスである請求項２３記載のコンピュータ使用メーター。

２５．さらに、オペレーティング・システム・メッセージを傍受し、オペレーティング・システム・メッセージモジュールに応答する予め定められたタイプのメッセージの受信を示すステップを含んでいる請求項２３記載のコンピュータ使用メーター。

【発明の詳細な説明】

コンピュータ使用メーターおよび解析装置

発明の背景

1．発明の分野

本発明は、コンピュータの使用状態を監視するシステムに関し、特にパーソナルコンピュータで予め選択された動作を収集し、記録し、解析し、使用状態の傾向を報告するシステムに関する。

2．関連技術の説明

パーソナルコンピュータの人気は、この１０年の間に爆発的に高まった。パーソナルコンピュータの利用人口は、使用されるパーソナルコンピュータ数やその使用方法と共に年々増加している。この急速な拡大の結果、コンピュータ、コンピュータ関連サービス、コンピュータソフトウェア、コンピュータ周辺装置、および電子情報ならびに情報サービスに使われた金額は、天文学的に増大している。わずか数年のあいだに、コンピュサーブ(CompuServe)，Prodigy，およびアメリカ・オン・ライン(America On-Line)のようなオン・ラインサービスが仮想上の不可解な言葉から周知の言葉になった。子供たちは自転車に乗ることができる前に、“ネット”をサーフすることを学ぶ。これまで、構内または広域ベースでコンピュータの使用度を測定するための効率的で信頼性の高いメカニズムがなかった。

任意のコンピュータ関連の製品あるいはサービスを販売している、または任意の電子フォーマットで任意の市場取引き活動を行っている組織体の間において、コンピュータ関連のリソースの使用状態や電子情報の普及状況を測ることが強く求められている。テレビ市場を評価するためにテレビ広告主が視聴率や視聴者デモグラフィに頼るのと全く同様に、“電子”広告主および売り手、コンピュータ関連製品およびサービスの製作者はコンピュータの使用状態および“オン・ライン視聴率”に関する情報を評価することを必要としている。

発明の概要

本発明の目的は、パーソナルコンピュータのソフトウェアの使用状態に関する

信頼性の高い情報の収集を容易にすることである。

本発明の別の目的は、商業的オン・ラインサービスの高い信頼性のマルチ・メディア視聴統計値を収集し、かつインターネットのワールド・ワイド・ウェブ(World Wide Web)を含む“情報スーパーハイウェイ”へのアクセスを容易にすることである。

本発明のさらに別の目的は、それに限定されるものではないがソフトウェア製造業者、商業オン・ラインサービスのプロバイダ、コンピュータ・ハードウェア製造業者、およびオン・ライン販売者を含む多数の異なる産業部門にとって有効な報告書を作成するためにパーソナルコンピュータを使用している世帯のパネルの設立を容易にすることである。

本発明によると、オペレーティング・システム・メッセージを受けて、監視するシステムが提供されることができる。このようなメッセージは、目標を定められた種々のアプリケーションへの指令でもよいし、或はオペレーティング・システムのオーバーヘッド・メッセージであってもよい。このようなメッセージは、マイクロソフト(Microsoft Windows)オペレーティング環境のようなオペレーティング・システムソフトウェアによって内部で生成されてもよい。本発明によるシステムは、膨大なメッセージアレイをフィルタし、あるアプリケーションから別のアプリケーションへの集中的な(in focus)変化を示すメッセージのような特定のメッセージだけを捕捉することができる。これらの集中的な変化は、アプリケーション始動、アプリケーションの終了、あるアプリケーションから別のアプリケーションへのリソースの切替え、アプリケーションの最小化、またはアプリケーションの復元を含んでもよく、またこれらに限定されない。

本発明によると、オペレーティングシステム・メッセージを受けることが可能であり、適切なメッセージをその他の関連した、または有効な情報と共に、ログファイルに記録することができる。このような関連のある、または有効情報は、日付スタンプ、時刻スタンプや、始動、終了、スイッチ、最小化、復元のようなメッセージタイプ、世帯ＩＤ番号、世帯内の個人ユーザーの識別、アプリケーションの実行可能なプログラムファイル名とファイル寸法の識別、アプリケーショ

ンのウインドウタイトル、およびそのアプリケーションの“インスタンス”へのハンドルを含んでいる。世帯識別番号は、世帯の“パネル”内のパーソナルコンピュータを特有に識別する番号であってよく、各パーソナルコンピュータがローカル・測定システムを使用することによってデータをシステムに提供している。

本発明によるシステムは、複数のコンピュータおよびコンピュータユーザーと共同して使用できる点が有効である。このシステムと結び付けられたコンピュータおよびコンピュータユーザーは、はるかに広範囲のユーザーを表すように意図されてもよい。これは、限定された世帯数に基づいてテレビジョン視聴率を設定するために使用されるテレビジョン視聴情報の収集に類似している。限定された世帯数は、全体的なコンピュータの使用または“視聴”を表すものと考えられる。

本発明によると、パーソナルコンピュータ中に設置されたメーターアプリケーションは、任意の所定のアプリケーションの一番上のウインドウに対する事象をログファイルに記録することができる。アプリケーションの子ウインドウに固有の事象は、必ずしもログファイルに書込まれなくてよい。ある特定のアプリケーションに対しては、このような子ウインドウに対する追加的な詳細な事象のログファイル書込みが発生するであろう。あるアプリケーションがさらに詳細なログファイル書込みの目標とされた場合、子ウインドウの生成を示すメッセージがログファイルに記録されるであろう。ログファイル中の項目は、少なくとも日付、時刻、世帯ＩＤ番号、コンピュータを使用している世帯内の個人、親アプリケーションのインスタンスへのハンドル、親アプリケーションの現在のウインドウタイトル、および子ウインドウタイトルを含んでいることが有効である。

さらに本発明の目的は、ある特定の外部通信を監視して、ログファイルに記録することである。ローカル・メーターアプリケーションは、モデムのような通信ポートに送られた文字のストリングを監視する。システムはある予め定められた文字ストリングを監視して、このようなストリングの発生時にある情報をログファイルに書込むように設定されてもよい。例えば、システムがストリング“ｈｔｔｐ：”を検出した場合、このシステムは、次に続くものがインターネットのワールド・ワイド・ウェブ上のハイパーテキスト・プロトコルサイトに対するユニ

バーサル・リソース・ロケータ（ＵＲＬ）の残りのものであることを認識する。

ローカル・メーターアプリケーションがＵＲＬを識別した場合、それは全ＵＲＬを受けてログファイルに書込む。この状況において、ログ項目は、少なくとも日付、時刻、世帯ＩＤ番号、その世帯内の個人ユーザー、親アプリケーションのインスタンスへのハンドル、親アプリケーションの現在のウインドウ・タイトル、およびユニバーサル・リソース・ロケータ（ＵＲＬ）を含んでいてもよい。

本発明によると、アプリケーションはまた特別のログを作成し、または特別の事象をログファイルに書込んでもよい。これらの特別のログ／事象は、予め選択されたアプリケーション或はアプリケーションの、オンライン・サービスあるいはインターネットブラウザのリクエストのようなクラスに焦点を合わせてもよい。パーソナルコンピュータの焦点となる周期的な監査をトリガーするために、タイマーが使用可能である点が有効である。周期的な監査は、例えば１／２秒ごとに、または適切な別のインターバルで行われてもよい。このインターバルは、焦点となるものの移行をミスする危険を冒すという犠牲を払って処理リソースを節約するためにもっと長い期間であってもよい。

本発明の１つの特徴によると、周期的な監査は、予め選択されたアプリケーションが実行しているか否かを決定するために開いているウインドウの全てに対してオペレーティングシステムにポーリングしてもよい。このような予め選択されたアプリケーションは、アメリカ・オンライン（America On-line）、Prodigy、マイクロソフトネットワーク(Microsoft Network)、はコンピュサーブ(Compuserve)のようなオン・ラインサービス・アプリケーションを含んでいてもよい。このようなアプリケーションが実行されている場合、メーターアプリケーションは、アプリケーションのタイトル・バーとこのようなアプリケーションの中の一番上のウインドウとのテキスト内容をログファイルに書込んでもよい。アプリケーションのタイトル・バーまたは一番上のウインドウのテキスト内容が前の監査から変化した場合にだけ、システムはタイトル・バーをログファイルに書込むことが有効である。さらに、各監査は編集ボックスのために開いているウインドウを監視してもよい。開いているウインドウ中に編集ボックスを見出だすと、シス

テムは、それがＵＲＬと一致しているか否かを決定するために編集ボックスの内容のシンタクスを検査する。一致している場合、ＵＲＬは事象ログまたは特別のログに書込まれることができる。

本発明によると、メーターアプリケーションは、コンピュータ上にメーターアプリケーションをインストールするための機構、データ記録のためのデータ圧縮および暗号化システム、ログ転送機構、自己更新ソフトウェア特徴、およびユーザーを含むその他多数の“ハウスキーピング”特徴を有していてもよい。

データ圧縮および暗号化システムは、事象ログの記憶に割当てられなければならないメモリリソースを最小にするために設けられていることが有効であり、またそこに含まれている情報のセキュリティを高めるために事象ログを暗号化してもよい。

データ転送システムは、ローカル・パーソナルコンピュータ使用ログを中央処理システムに転送するために設けられることができる。中央処理システムは、多数のローカル・パーソナルコンピュータ使用ログを取り入れ、ログ情報を有効な情報に変換し、情報を評価して、コンピュータ使用状態の種々の報告書や解析結果を作成してもよい。この転送は、自動化され、ユーザーにより開始された、或は中央局により開始された電子転送、或はディスケットのような磁気記憶媒体への局部的ダウンローディング、および中央処理位置へのディスケットの転送を含む多数の異なる機構の任意のもので行われてもよい。

コンピュータ使用メーターおよびその支援ソフトウェアは、時々システム更新を経験する可能性がある。これらの更新は、ソフトウェアに特徴を付加して、どのようなシステムバグでも修正するように意図される。各パネリストは、前の月のログファイルに書かれた活動を収集することを目的として、月に１度が有効な固定したサイクルで連絡を取ってもよい。このプロセスは、パネリストに郵送された、或はモデムを介して電送されたディスケットにより行われてもよい。どのような媒体ででも転送されるデータ転送プログラムは、最初に任意の顕著なソフトウェア・アップグレードを調べることができる。あるものがスケジュールされている場合には、ソフトウェアがパネリストのコンピュータに自動的に転送され

る。

システムは、アプリケーションのタイプであるソフトウェアの特定のクラスの使用後などのある環境にかかわるアンケートを含んでもよいし、或は事象ログまたは別のファイルに記憶されていてもよい所望の情報を入力するようにユーザーが周期的にプロンプトされてもよい。データ転送システムは、回答をアップロードし、また追加された質問またはトリガーをダウンロードするために使用されてもよい。

本発明によるシステムの利点の1つは、事象ログにおけるプロセッサ注目度の変化を記録することである。ソフトウェアの販売者は、ユーザーの彼等の製品に対する反応についての情報を強く希望している。もしこれを行うとすれば、典型的にペーパーアンケートまたは電話を通してのインタビューにより“使用”情報が収集される。このような状態では、回答者は対象となる彼等自身の製品の使用を思い出すように求められる。このテクニックは、人間の記憶力に固有の限界と不正確さ、個々のコンピュータユーザーがこのような情報を提供するために費やすことをいとわない時間量の限界、およびアンケートに返答する個人がコンピュータシステムを使用する世帯のメンバーの1人だけであるかもしれず、関連のある情報の全てを有していない可能性があることを含む重大な欠陥を示す。

本発明によるシステムは上述の欠点を克服する。最初の設置プロセスの後、システムは完全に受動的になってもよい。すなわち、コンピュータユーザーは、システムを効率的に動作させるための付加的なアクションを取る必要はない。任意のソフトウェア製品またはアプリケーションプログラムを使用することにより、システムにより記録されたオペレーティングシステム環境中の事象メッセージが自動的にトリガーされる。この自動方式により、コンピュータユーザーとの後続的な対話よりはるかに多くの情報がコンピュータによって収集されることができる。例えば、ある事象の日付および時刻に関する情報は、コンピュータの内部クロックとカレンダーを使用して容易に獲得されてもよく、ここにおいてこのような情報は、後の個人的な報告の間にユーザーによって通常思い出されないものである。事象ログの構造は、典型的に有効な情報に非常に富んでおり、少なくとも

ソフトウェア・タイトルによるソフトウェア使用分類や、ソフトウェアのサブカテゴリィ（例えば、スプレッドシート、スクリーンセイバー、通信ソフトウェア、個人情報管理、ワードプロセッサ等）の分類、または例えば子供の有無、収入、家の間取り等の世帯デモグラフィによる分類を可能にする。本発明によるシステ

ムはまた、分単位による合計使用時間、すなわち分単位による累積集中時間、使用頻度すなわち所定の時間フレーム中のアクセス数、およびコンピュータ使用のシェアによってソフトウェアの使用量を測定することができる。

有効な付加的な特徴によると、システムはある特定のアプリケーションをログファイルに詳細に記録することを可能にする。商業的なオン・ラインサービス業界は非常に競争的であり、またマイクロソフト社の参入により、その競争率が高まるであろう。現在、コンピュサーブ、Prodigyおよびアメリカ・オンラインという大手３社のプロバイダが、それぞれ約２百万人の加入者を有している。これらの組織体にとって唯一最大の問題は、加入者の自然減を減らし、かつ任意の個人が定期利用契約を継続する期間を長くすることである。実際、加入者の減少は顧客の満足度の尺度であり、逆の立場から言えば、それはオンライン・サービスの収入傾向と関係している。このような減少を減らすことは、加入者をより長期間にわたって確保し、かつ収入を増加するということを意味する。

本発明によるシステムは、商業的なオン・ライン・サービスのプロバイダやユーザーアプリケーションのために子ウインドウ情報を収集することができる点が有効である。これらのアプリケーションの子ウインドウのウインドウ・タイトルは、一般にその瞬間における活動の役に立つ記述を有している。例えば、加入者がそのサービス用のメールシステムを使用している場合、このウインドウ・タイトルがそのように示す。本発明によるシステムは、ログファイルにこれらのタイトルを記録する。

例示すると、電子メールメッセージを書込むためのウインドウのウインドウタイトルは、コンピュサーブでは“メールを書きなさい”であり、Prodigy では“書込め”であり、またアメリカ・オンラインでは“メールを作成せよ”である。

この情報の収集と解析は、競争的なサービスの種々の特徴に費やされた時間の分布、それぞれの特徴のいずれが多数のサービスのユーザーによって好まれたかの識別、および種々のサービスのいずれの特徴の人気が高いかの識別、およびこれらの特徴への注目度が加入契約期間の長さと関連して変化する状態を含み、それらにだけ限定されないが、多くの点でオン・ラインのサービスプロバイダにとって貴重である。ログに記録された情報は、顧客についての直接的なフィードバックをオン・ラインサービスのプロバイダに提供し、かつサービスを改良すべきエリアを指摘することができるので、プロバイダにとって貴重である。本発明によるシステムはまた、電子マガジンや新聞のような商業的なオン・ラインサービスのオン・ライン内容エリア内のトラフィックを測定することができる。出版業者がオン・ラインメディアに進出すると、メディア・トラフィック統計値が重要になる。それは重要なデータをメディア立案者に提供する。さらに、本発明の有効な特徴は、通信ポートまたはモデムのトライックを傍受してログファイルへ記録する。商業的オン・ラインサービスに関する活動を追跡する延長として、本発明によるシステムは、それがまたインターネットのワールド・ワイド・ウェブのような他の通信チャネル上のトラフィックを測定した場合には、オン・ライン活動のフル・ピクチャーを作成することができる。ウェブ上のインターネット・サイトは、ユニバーサル・リソース・ロケータスキムによってアドレス可能である。

オン・ラインの販売者は、ウェブ・トラフィックの特徴を理解し、かつ異なるサイトでユーザーが費やす時間を把握しようとする。これらのトラフィック統計値は、コマーシャル時間の販売および価格決定の基礎としてテレビ視聴率を使用するのと同様に、メディア計画の基本データとなる。

付加的な有効な特徴によると、このシステムは、自動化されたファイル管理機能を含んでいる。これらの機能は、システムがホストコンピュータの効率的な動作を妨害することを阻止するために必要とされる。事象ログファイルは、非常に大きくなることができる。ログを可能な限り小さくしておくことが重要かもしれない。事象ログの大きさを減少するために、データ圧縮技術を使用してもよい。さらに本発明によるシステムは、可能な限り受動的なプロフィールを持続しなく

てはならない。したがって、自動化された設置およびデータ転送プログラムは、ユーザーのコンピュータ使用による妨害を減少させて、任意の特定のユーザーに対する影響を最小限にとどめる。

画面の簡単な説明

図１は、本発明のフロー図である。

図２は、本発明の１実施形態を示す。

図３は、メッセージおよび事象の転送を示す。

図４は、メッセージへの応答を示す。

図５は、監査ベースのサブシステムを示す。

好ましい実施形態の詳細な説明

本発明の１実施形態によると、パーソナル・コンピュータ・リソースの使用に関する情報を収集し、処理して転送するシステムが提供される。図１は、本発明による１実施形態のフロー図を示す。コンピュータ使用メーター１は、パネリストまたはユーザーのグループ10によって所有され、および、または動作されるパーソナル・コンピュータの上に設置されてもよい。パネリストは有効に特定の世帯のメンバーを指し、また１人以上の個人から構成されてもよい。コンピュータ使用メーターは、有効に事象ログファイル11を生成する。機構２は、中央処理ステーションに事象ログファイルを転送するために設けられている。この転送は、フロッピーディスクのような可搬性の媒体への転送によって、または電話リンクのような通信チャネルを介して、或は電子メールによって行われてもよい。転送は、時間、ログファイルに書込まれた事象の数、ログファイルの大きさ、使用された、または利用可能なリソース、或はそれらの任意の組合わせのような任意の予め定められた基準によって行われてもよいし、或はトリガーされてもよい。中央処理ステーションは、複数の別個のコンピュータ使用メーター12からのログファイルを蓄積する。位置３における中央処理ステーションは、複数の事象ログファイルからの情報を有しているデータベース13をロードする。中央処理ステーションはマイクロプロセッサベースのコンピュータであってもよいし、またコンピュータ使用データベース13を管理し、カスタム化されたデータ辞書14を作成する

ために種々の市販の、および、またはユーザー独自に作成したデータベース管理システム４を使用してもよい。カスタム化されたデータ辞書は、事象ログファイルによって供給された生データを解釈するために設けられている。さらに、データベース管理システム４は、有効な情報を抽出し、予備処理および／または蓄積された事象ログファイルの解析を行ってもよい。このシステムはまた位置15において使用データを識別する。カスタム化された辞書によって認識されない、ログファイルに書込まれている任意の事象は、例外として認識され、その後の手動式の識別のために記憶される。この段階でのユーザーまたは手動式の介在は、それ

以上の識別を可能にし、またカスタム化された辞書14は、類似した事象の後続的な発生がカスタム化された辞書14によって自動的に識別されるように更新されることができる。カスタム化された辞書または手動式の介在15のいずれかにより識別されたログ事象は全て、位置５において情報の生データベースを作成するために使用される。このデータベースは、異なるデータベース管理システムによって組織化されてもよい。データベースは、ＮＰＤグループ社から販売されているＮＰＤ／ＰＯＷＥＲＶＩＥＷデータベース16の形態のデータベースであることが意図されている。

位置６において、パワービュー(Powerview)データベース管理システムは、後続する解析７のためにデータベースにおいて報告または予備処理情報を生成してもよい。システムは、保持されたデータベース要素から生じた情報を示す報告を生成してもよい。データは組織化され、事実上任意の所望の方式および構成で報告されてもよい。種々の市販のデータベース管理システムが長所と短所を有しているとすれば、ハード・コピー報告17を生成するために、或はその場限りの解析または報告生成18のために使用可能なサブ・データベースを作成するために、データが１以上のデータベース管理システムによって処理されてもよい。

図２は本発明によるコンピュータ使用メーターを示し、ウインドウズ(Windows)環境で動作しているＩＢＭ適合パーソナル・コンピュータにインストールされた情報およびデータ流を表している。ウインドウズ環境は、種々のモジュールによって使用されるメッセージを内部で生成し、コンピュータのオペレーションを

管理し、そのリソースを割当てる。ほとんどのアプリケーション・プログラム作成には、オペレーティング・システムによって処理される内部オーバーヘッドによる処理が不要である。ウインドウズ環境は、内部駆動装置を使用することによって膨大なオーバーヘッド機能アレイを処理する。内部駆動装置はウインドウズ・キーボード駆動装置20およびウインドウズ・マウス駆動装置21を含んでいてもよい。これらの駆動装置は、オーバーヘッドがマウスポインタを操作し、マウスボタンをクリックし、またキーボード上で情報を入力するのを管理する。マウス事象やキーボード事象のようなユーザ・インタフェース事象は、ウインドウズ・ユーザー・モジュール22に転送される。

図２に示されているように、コンピュータ使用メーターの主要動作モジュール23はＲＩＴＡとして示されされており、それ自身のウインドウ内で動作する。ウインドウズ・ユーザー・モジュール22は、WM__ＣＲＥＡＴＥ、WM__ＳＹＳＣＯＭＭＡＮＤ、WM__ＣＯＭＭＡＮＤ、WM__ＱＵＥＲＹＥＮＤＳＥＳＳＩＯＮ、およびWM__ＤＥＳＴＲＯＹのようなアプリケーション・特定メッセージを生成する。これらのメッセージは特定の主ウインドウ・アプリケーション・モジュールだけに使用されるように意図されている。ＲＩＴＡモジュール23は、ＲＩＴＡアプリケーション・主ウインドウ23を呼出す命令のためにこれらのメッセージを監視する。ＨＯＯＫＳ　ＤＬＬモジュール24は、呼出された後、ＲＩＴＡ主ウインドウ・モジュール23にメッセージを与えるように動作する。パーソナル・コンピュータの動作中、ウインドウズ・ユーザー・モジュール22は、ウインドウズ・コール・バックまたは“ＣＢＴ”事象を生成する。ある特定の事象はＨＯＯＫＳ　ＤＬＬモジュールにより傍受され、ＲＩＴＡ主モジュール23に転送される。ＲＩＴＡ主ウインドウは、このようなメッセージを受取ると、ある特定のメッセージをＲＩＴＡログファイル記録サブシステム24に送る。さらに、ＲＩＴＡ主ウインドウ23は、ＲＩＴＡ　ＩＮＩファイル・サブシステム25にプログラム実行時間パラメータを転送する。このＲＩＴＡ　ＩＮＩファイル・サブシステム25は、パネリスト名を収集するためにパネリスト情報ダイアログ・ボックス26と通信する。このパネリスト情報ダイアログ・ボックス26はまた、ＲＩＴＡ主ウインドウ

23に活動的なユーザー名を転送する。活動的なユーザー名は、ログファイル記録動作に関連して使用される。

図３は、ウインドウズＣＢＴ事象およびウインドウズ・ユーザー定義メッセージの転送を示す。ウインドウズ・ユーザー・モジュール22がＨＣＢＴ＿ＡＣＴＩＶＡＴＥメッセージを生成すると、このようなメッセージはＨＯＯＫＳ　ＤＬＬモジュールによって認識され登録される。ＨＣＢＴ＿ＡＣＴＩＶＡＴＥは、現在活動的なウインドウと、始動させられようとしているウインドウの識別を表す。ＨＯＯＫＳ　ＤＬＬモジュールは、ＨＣＢＴ＿ＡＣＴＩＶＡＴＥを受取ると、ＷＨ＿ＨＣＢＴ＿ＡＣＴＩＶＡＴＥをメッセージを送って、始動させられているウインドウのＲＩＴＡによるログファイルへの書込み用のハンドルを示す。このハンドルは、マイクロソフト・ウインドウズの活動的なプロセスを固有に識別した整数である。ウインドウズ・ユーザー・モジュール22から新たに作られたウインドウのハンドルを示すＨＣＢＴ＿ＣＲＥＡＴＥＷＮＤメッセージを傍受すると、ＨＯＯＫＳ　ＤＬＬモジュール24は、ログファイルに記録するためにＷＨ＿ＨＣＢＴ＿ＣＲＥＡＴＥＷＮＤをＲＩＴＡに送る。破壊されようとしているウインドウのハンドルを示すウインドウズ・ユーザー・モジュール22からのＨＣＢＴ＿ＤＥＳＴＲＯＹＷＮＤメッセージを傍受すると、ＨＯＯＫＳ　ＤＬＬモジュール24は、ログファイルに記録するためにＷＨ＿ＨＣＢＴ＿ＤＥＳＴＲＯＹＷＮＤメッセージをＲＩＴＡ主ウインドウ23に送る。最小化または最大化されようとしているウインドウのハンドルを示すウインドウズ・ユーザー・モジュール22からのＨＣＢＴ＿ＣＢＴ＿ＭＩＮＭＡＸメッセージを傍受すると、ＨＯＯＫＳ　ＤＬＬモジュール24は、ＷＨ＿ＨＣＢＴ＿ＣＢＴＭＩＮＭＡＸメッセージをＲＩＴＡ主ウインドウ23に送る。ＨＣＢＴ＿ＣＢＴＭＩＮＭＡＸメッセージは、それぞれがウインドウが最小化されている、最大化されている、復元されているかどうかを示す動作コードであるいくつかの形態を取ることができる。受信された動作コードに応じて、ＨＯＯＫＳ　ＤＬＬモジュール24は、ＳＷ＿ＨＩＤＥ、ＳＷ＿ＳＨＯＷＭＩＮＩＭＩＺＥＤ、ＳＷ＿ＭＩＮＩＭＩＺＥ、ＳＷ＿ＲＥＳＴＯＲＥ、ＳＷ＿ＭＡＸＩＭＩＺＥ、ＳＷ＿ＮＯＲＭＡＬ、またはＳＷ＿ＳＨＯＷを含むいくつ

かのメッセージの1つをログファイルに書込むためにＲＩＴＡに送る。

図4は、ウインドウ・ユーザー・モジュール22によって生成されたウインドウズ・アプリケーション・メッセージに対するＲＩＴＡEウインドウ23の応答を示す。ブロック27は、WM__ＣＲＥＡＴＥメッセージに対するＲＩＴＡ応答を示す。WM__ＣＲＥＡＴＥメッセージは、アプリケーションがスタートしていることを示す。応答がパネリストＩＤメッセージをプロンプトし（これが最初ならば、アプリケーションが実行される）、ＭＥＴＥＲ動作コード項目をログファイルに書込み、ＰＡＮＥＬ動作コード項目をログファイルに書込み、ＳＴＡＲＴ動作コード項目をログファイルに書込み、1以上のＲＵＮＮＧタスク項目をログファイルに書込む。パネリストＩＤに対するプロンプトは、パネリストが予め定められた7桁の番号により独自の識別を可能にする。以下に説明するように、ログファイ

ルに書込まれた各事象にはログ項目の構成が必要である。各項目は、ログファイルに記録されている事象のタイプを示す動作コードを含む。ＲＵＮＮＧタスク項目は、コンピュータ使用メーターが主ＲＩＴＡモジュールにより呼出されたときに、既に動作しているどのウインドウズ・アプリケーションに対してでもログファイルに書込まれる。ブロック28は、WM__ＳＹＳＣＯＭＭＡＮＤメッセージに対するＲＩＴＡ応答を示す。WM__ＳＹＳＣＯＭＭＡＮＤメッセージは、ユーザーがウインドウズ・デスクトップからＨＴＩアイコンを付勢させたことを示す。応答によって、ユーザー・ダイアログを変更し、ＰＡＮＥＬ動作コード項目をログファイルに書込む。ユーザー・ダイアログの変更は、次のログファイルに書込まれたレコードに記憶されたユーザ名に影響を与える。ブロック29は、WM__ＱＵＥＲＹＥＮＤＳＥＳＳＩＯＮメッセージへのＲＩＴＡ応答を示す。WM__ＱＵＥＲＹＥＮＤＳＥＳＳＩＯＮメッセージにより、ウインドウズはシャットダウンしているが、それがきちんとそれ自身を閉じるように、最初にＲＩＴＡに制御を渡すことを示す。応答によって、ＳＴＯＰＭ動作コード項目をログファイルに書込み、ログをクリアする。ブロック30は、ユーザー・モジュールによって生成されたWM__ＤＥＳＴＲＯＹメッセージに対するＲＩＴＡ応答を示す。WM__ＤＥ

ＳＴＲＯＹメッセージは、ユーザーが明確にＲＩＴＡを閉じたことを示す。この応答によって、ＳＴＯＰＭ動作コード項目をログファイルに書込み、ログをクリアする。ログ・クリア動作は、メモリに依然として保持されている任意のレコーをログファイルに書込むことから成る。

ログファイルは、データを記憶するために固定したコラムフォーマットを使用してもよい。最初のコラムは、ポストプロセッサの文解析のために使用されることのできるロギング・シーケンス番号を含んでもよい。ログファイルはまた、日付スタンプおよび時刻スタンプが各レコードに与えられるコラムを含んでいてもよい。次のコラムは、以下のような動作コードを含んでいてもよい：

ＲＵＮＮＧ　これは既に実行しているタスクを示す
ＰＡＮＥＬ　パネリスト名および識別が記録データ部分に配置される
ＭＥＴＥＲ　アプリケーション・ログおよびバージョン情報

ＳＴＡＲＴ　メーターをスタートする
ＡＣＴＶＴ　一番上のウインドウ・タスクが始動させられたことの記録
ＴＳＴＲＴ　一番上のウインドウ・タスクがスタートしたことの記録
ＴＳＴＯＰ　一番上のウインドウ・タスクがストップしたことの記録
ＭＩＮＩＭ　一番上のウインドウが最小化されたことの記録
ＲＥＳＴＯ　一番上のウインドウがそのアイコン状態から復元または最大化された状態からその元の状態に復元されたことの記録
ＳＴＯＰＭ　メーターをストップする
ＩＮＴＲＶ　レコード・データをインタビューする

以下にログ項目の一例を示す。

00001	05/25/95	10:40:27	METER	1234561 0000	[D=02.00-02]
00002	05/25/95	10:40:27	PANEL	1234561 0000	[D=John Doe]
00003	05/25/95	10:40:27	START	1234561 0000	[D=ini StartTask=1 EndTask=1 Minimize=2 Maximize=1 Activate=1 Restore=1 Running=1]
00004	05/25/95	10:40:27	RUNNG	1234561 2a96	[D=C:\DOS\MOUSE\POINTS R.EXS] [T=Pointer Options] [S=10432]
00005	05/25/95	10:40:27	RUNNG	1234561 201e	[D=C:\WINDOWS\NETDDE.E XS] [T=NetDDE] [S=§2432]
00006	05/25/95	10:40:27	RUNNG	1234561 1f6e	[D=C:\WINDOWS\SYSTEM\ DDEML.DLL] [S=39424]
00007	05/25/95	10:40:27	RUNNG	1234561 0736	[D=C:\WINDOWS\SYSTEM\ USER.EXE] [S=264096]
00009	05/25/95	10:40:27	RUNNG	1234561 37de	[D=C:\HTI\HTI.EXE] [T=HTI] [S=55656]
000010	05/25/95	10:40:27	MIMIM	1234561 37de	[D=C:\HTI\HTI.EXE]
000011	05/25/95	10:40:28	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH. EXE]
000014	05/25/95	10:40:29	TSTRT	1234561 357e	[D=C:\APPWIN\OMGUI\ OMGUI.EXE] [T=OpenMail user 'pinsley' on server 'ny!'] [S=443360]
000015	05/25/95	10:40:33	TSTRT	1234561 36d6	[D=C:\WINDOWS/UALALLOC. EXE] [S=3776]
000016	05/25/95	10:40:33	TSTRT	1234561 08cc	[D=C:\WINDOWS\SYSTEM\ HSASRV.EXE] [T=Windows Sockets Asynchronous Request Server] [S=6505]
000017	05/25/95	10:40:34	TSTOP	1234561 357e	[D=C:\APPWIN\OMGUI\OMG UI.EXE]
000018	05/25/95	10:40:34	TSTRT	1234561 357e	[D=C:\APPWIN\OMGUI\OMG UI.EXE]

000019	05/25/95	10:40:34	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000022	05/25/95	10:40:36	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000024	05/25/95	10:40:36	TSTOP	1234561 1f6e	[D=C:\WINDOWS\SYSTEM\DDEML.DLL]
000025	05/25/95	10:40:36	TSTOP	1234561 1f6e	[D=C:\WINDOWS\SYSTEM\DDEML.DLL]
000026	05/25/95	10:40:40	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000027	05/25/95	10:40:40	TSTRT	1234561 2fe6	[D=C:\WINDOWS\CALC.EXE] [T=Calculator] [S=45072]
000028	05/25/95	10:40:41	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000029	05/25/95	10:40:43	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000030	05/25/95	10:40:43	TSTRT	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE] [T=Cardfile - (Untitled)] [S=93184]
000031	05/25/95	10:40:44	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000032	05/25/95	10:40:46	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000033	05/25/95	10:40:46	TSTRT	1234561 2b16	[D=C:\WINDOWS\NOTEPAD.EXE] [T=Notepad - (Untitled)] [S=32736]
000034	05/25/95	10:40:46	ACTVT	1234561 2b16	[D=C:\WINDOWS\NOTEPAD.EXE]
000035	05/25/95	10:40:51	ACTVT	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000036	05/25/95	10:40:57	ACTVT	1234561 2fe6	[D=C:\WINDOWS/CALC.EXE]
000037	05/25/95	10:40:58	MINIM	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000038	05/25/95	10:40:58	ACTVT	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000039	05/25/95	10:41:00	ACTVT	1234561 2b16	[D=C:\WINDOWS\NOTEPAD.EXE]
000040	05/25/95	10:41:02	TSTOP	1234561 2b16	[D=C:\WINDOWS\NOTEPAD.EXE]

000041	05/25/95	10:41:02	ACTVT	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000042	05/25/95	10:41:04	ACTVT	1234561 2fe6	[D=C:\WINDOWS/CALC.EXE]
000043	05/25/95	10:41:05	RESTO	1234561 2fe6	[D=C:\WINDOWS/CALC.EXE]
000044	05/25/95	10:41:06	TSTOP	1234561 2f36	[D=C:\WINDOWS/CALC.EXE]
000045	05/25/95	10:41:06	ACTVT	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000046	05/25/95	10:41:08	TSTOP	1234561 3016	[D=C:\WINDOWS\CARDFILE.EXE]
000047	05/25/95	10:41:08	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000048	05/25/95	10:41:16	ACTVT	1234561 164e	[D=C:\APPWIN\DASH\DASH.EXE]
000049	05/25/95	10:41:19	STOPM	1234561 0000	[D=Windows Shutdown]

ログ項目表に示されているように、各項目は、シーケンス番号、日付スタンプ、時刻スタンプ、動作コードまたは事象タイプと、データフィールドを含む。データフィールドに含まれている情報は、事象タイプによって指図される。示されている例において、次のフィールドは、パネリストまたはユーザー識別、この場合は、存在するならばアプリケーションのインスタンスへのハンドルを含むフィールドにより後続される“１２３４５６１”を含む。ログレコード・シーケンス番号０００００１は、データフィールド中にアプリケーション、ロゴおよびバージョン情報を記録するメーター動作コード項目を有している。シーケンス番号０００００２を有するロゴ項目では、ＰＡＮＥＬ動作コードがパネリストの名前を記憶するように与えられ、それはまた別の識別情報を記憶してもよい。この例において、記録された名前はジョン・ドウ(John Doe)である。アプリケーションが始動させられると、コンフィギュレーション情報をデータフィールドに記録するＳＴＡＲＴ動作コードのログ項目が形成される。有効な実施形態によると、コンピュータ使用メーターは、始動の後に自動的に最小化される。その他の適切な情報が種々の事象タイプのログ項目のデータ部分に含まれていてもよい。データフィールドは、ラベルによって識別される異なる情報を含んでいてもよい。示された例において、ラベル“Ｓ”はアプリケーションのファイル寸法を識別する。ラベル“Ｔ”は、アプリケーションのウインドウズ・タイトルを識別する。ラベル“Ｄ”は、

典型的にアプリケーションの全経路である、種々のデータを識別する。その他のラベルおよび情報もまたログファイルに書込まれることが可能である。

本発明の別の実施形態によると、使用メーターは、同じログファイルに、或は補助ログファイルのいずれかに付加的な事象を記録してもよい。付加的な事象は、周期的な監査に基づいてログファイルに書込まれることができる。周期的な監査は、タイマーによってトリガーされてもよい。そのタイマーはソフトウェアで実行されると有効であり、またそれ自身のウインドウの中で、或はシステムレベルで動作してもよい。監査は、その他のトリガー周期が選択されてもよいが、1／2秒ごとにトリガーされると有効である。使用メーターは、オン・ラインのプログラム活動に対してコンピュータ使用を周期的に監査してもよい。メーターは、予め定められた或いは予め選択されたコンピュータ・アプリケーション、またはモデムアクセスのような予め定められたリソースに頼るアプリケーションに対してコンピュータを監査するように設定されてもよい。予め選択されたコンピュータ・アプリケーションは、アメリカ・オンライン、コンピュサーブ、Prodigyまたはマイクロソフト・ネットワークによって提供される周知のオンラインサービス・アクセスと、インタフェース・アプリケーションであってもよい。予め選択されたアプリケーションの1つが表示されるか、或いはその代わりに始動させられていることが監査によって明らかにされた場合、アプリケーション・ウインドウと一番上のウインドウとからの情報がログファイルに書込まれる。ログファイルに書込まれた情報は、アプリケーションのタイトルバーのテキスト内容と、このようなアプリケーションの一番上のウインドウのテキスト内容であってもよい。好ましい改善によると、システムは、アプリケーションまたは一番上のウインドウのタイトルバーの内容が同じアプリケーションに対して前にログファイルに書込まれたタイトルバーと異なっている場合には、タイトルバーのテキスト内容だけをログファイルに書込む。

周期的な監査特徴の別の実施形態は、予め選択されたタイプの表示要素を周期的に監査することを含んでいる。ウインドウズ・オペレーティング・システムにおいて、それぞれ表示されたウインドウは、多数の表示要素で構成されている。この表示要素は、特に編集ボックスとボタンを含んでいる。好ましい特徴による

と、編集ボックスの内容は検査されることができる。内容が予め定められた基準と一致している場合、この内容はログファイルに書込まれる。例えば、編集ボックスの内容がＵＲＬに対するシンタクスと一致している場合には、ウインドウがインターネット・ブラウザ・プログラムに対応していると考えられる。編集ボックスの内容をログファイルに書込むということは、インターネット上の文書のユーザーのアクセスを示す。

図５は、監査ベースの使用メーターを示す。監査ベースのサブシステムはタイマー40を含んでいる。タイマー40は、監査モジュール41をトリガーする。監査モジュールは、監査ターゲット42の内容を予め定められた基準43と比較する。予め定められた基準が満足された場合、監査モジュールは、事象ログ44において項目を作成する。ターゲットは、コンピュータ使用と活動とを示す表示または他の情報であってもよい。基準43は、予め定められたアプリケーション・プログラム、ウインドウズ、または例えばインターネット、特にワールド・ワイド・ウェブ用のＵＲＬと一致したシンタクスのようなシンタクスの識別であってもよい。

当業者は、本発明による使用メーターが本発明の基本的な概念の範囲内において種々の方法で変更されてもよいことを理解するであろう。

【図１】

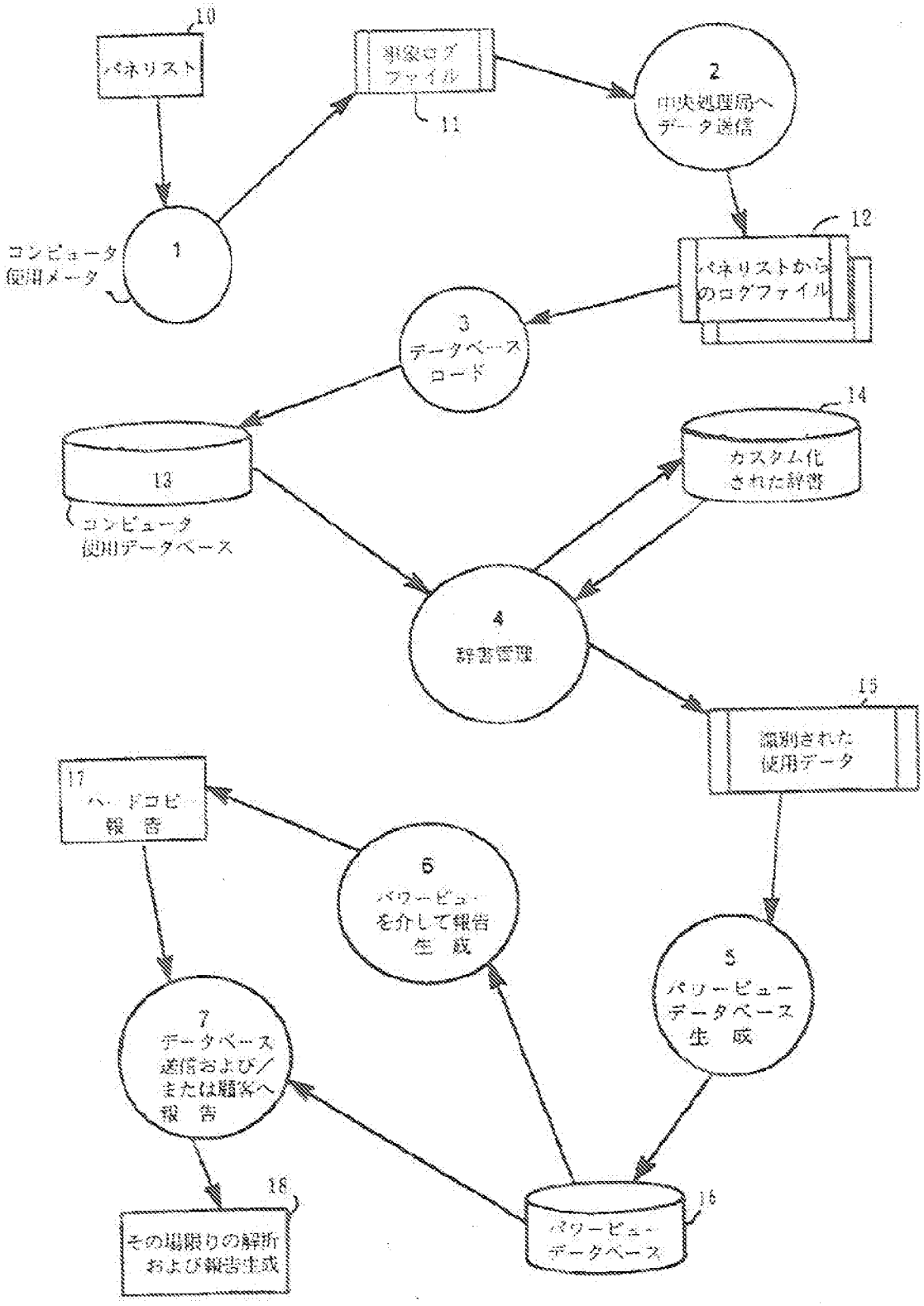
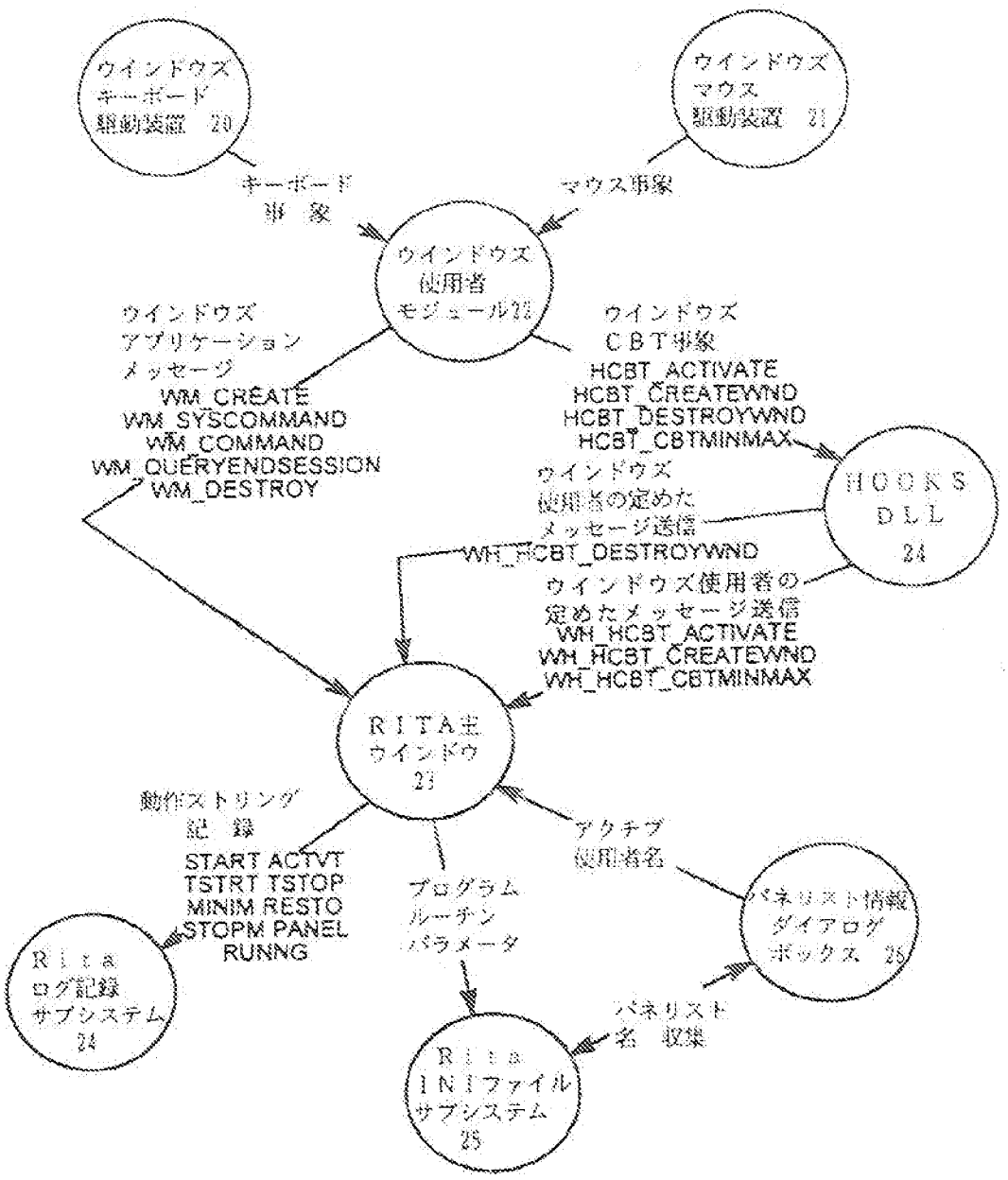

10
パネリスト
11
非ログファイル
2
中央処理局へデータ送信
12
パネリストからのログファイル
コンピュータ使用メータ
1
3
データベースコード
13
コンピュータ使用データベース
14
カスタム化された辞書
4
辞書管理
15
識別された使用データ
17
ハードコピー報告
6
パワービューを介して報告生成
5
パワービューデータベース生成
7
データベース通信および／または顧客へ報告
16
その場限りの解析および報告生成
16
パワービューデータベース

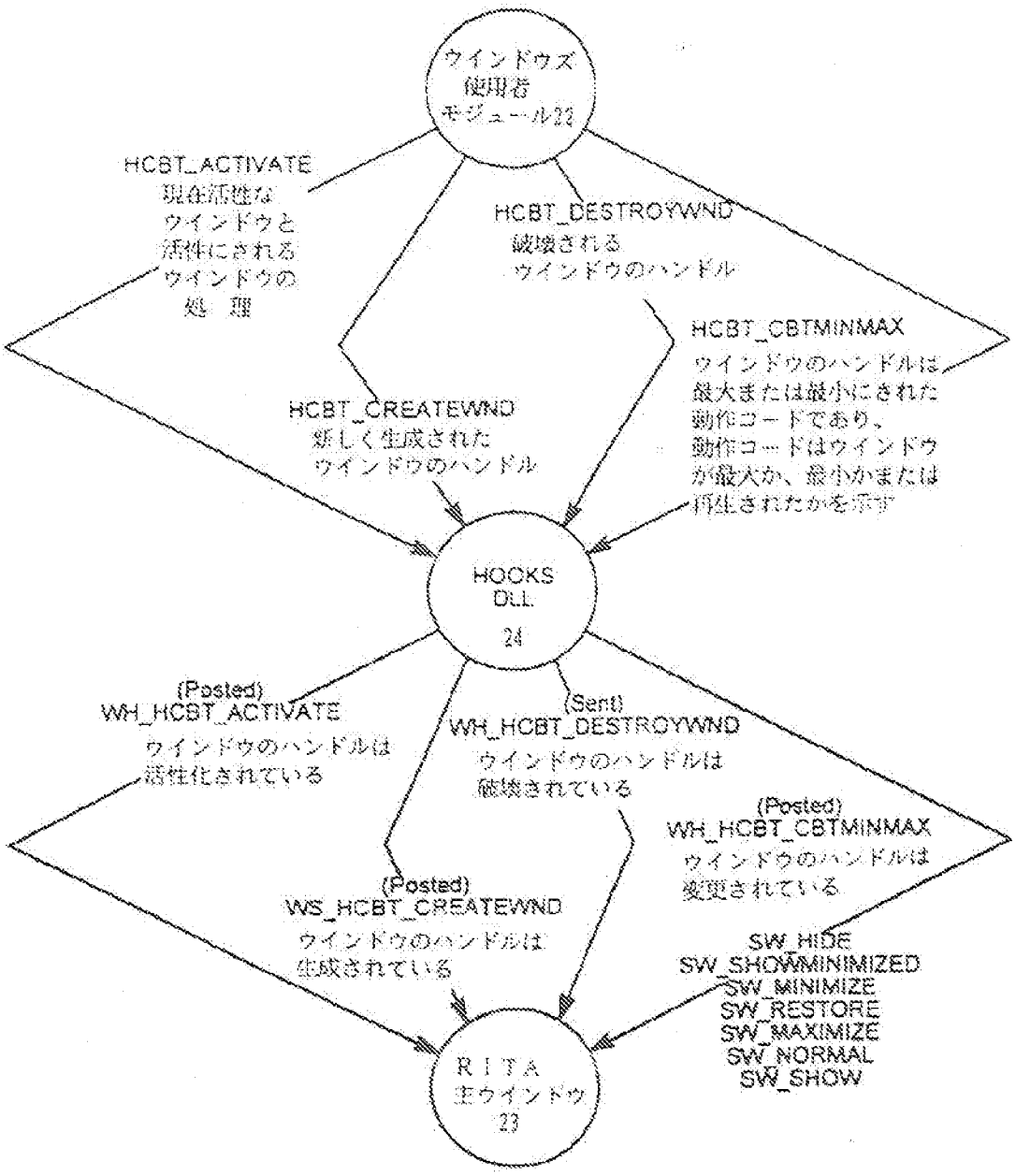
Figure 1

【図２】


ウインドウズ
キーボード
駆動装置 20
ウインドウズ
マウス
駆動装置 21
キーボード
事 象
マウス事象
ウインドウズ
使用者
モジュール23
ウインドウズ
アプリケーション
メッセージ
WM_CREATE
WM_SYSCOMMAND
WM_COMMAND
WM_QUERYENDSESSION
WM_DESTROY
ウインドウズ
ＣＢＴ事象
HCBT_ACTIVATE
HCBT_CREATEWND
HCBT_DESTROYWND
HCBT_CBTMINMAX
ＨＯＯＫＳ
ＤＬＬ
24
ウインドウズ
使用者の定めた
メッセージ送信
WH_HCBT_DESTROYWND
ウインドウズ使用者の
定めたメッセージ送信
WH_HCBT_ACTIVATE
WH_HCBT_CREATEWND
WH_HCBT_CBTMINMAX
ＲＩＴＡ主
ウインドウ
23
動作ストリング
記 録
START ACTVT
TSTRT TSTOP
MINIM RESTO
STOPM PANEL
RUNNG
プログラム
ルーチン
パラメータ
アクチブ
使用者名
パネリスト情報
ダイアログ
ボックス 26
パネリスト
名 収集
Ｒｉｔａ
ログ記録
サブシステム
24
Ｒｉｔａ
ＩＮＩファイル
サブシステム
25

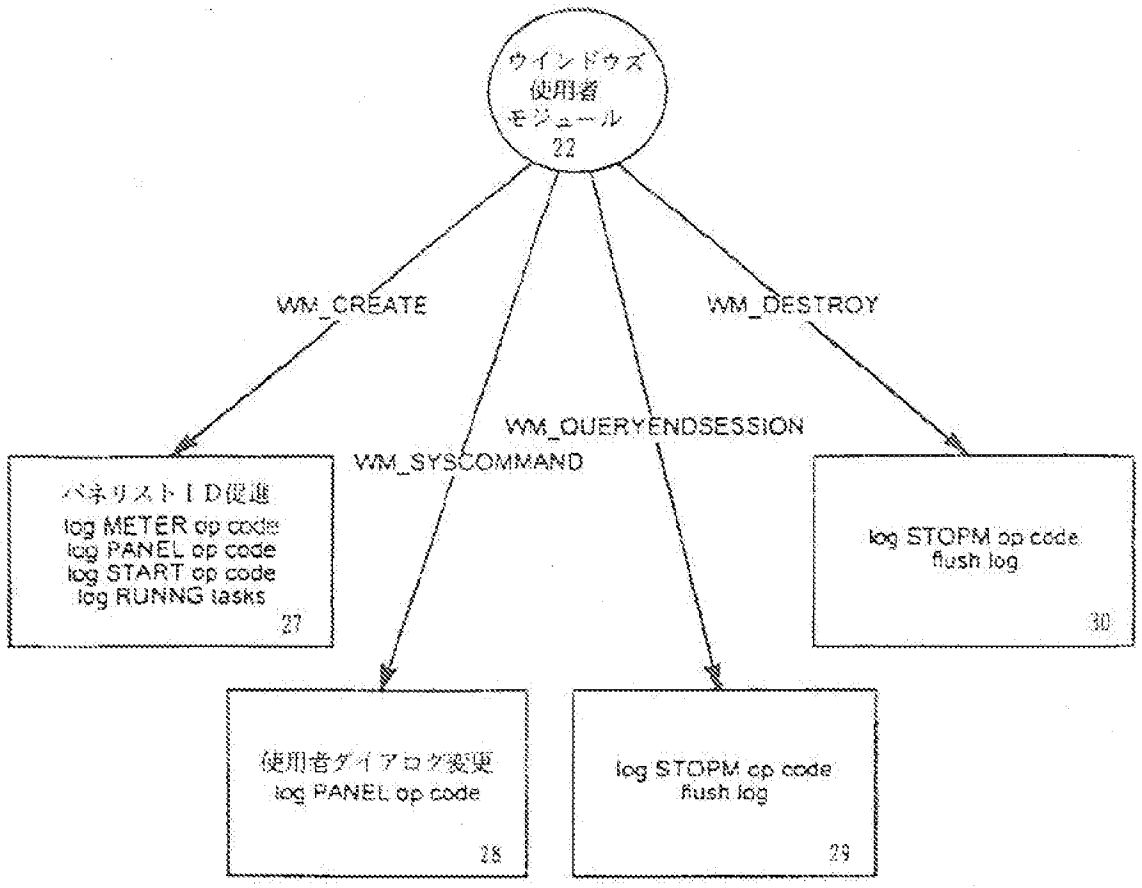
Ｆｉｇｕｒｅ２

【図３】


ウインドウズ
使用者
モジュール22
HCBT_ACTIVATE
現在活性な
ウインドウと
活性にされる
ウインドウの
処　理
HCBT_DESTROYWND
破壊される
ウインドウのハンドル
HCBT_CBTMINMAX
ウインドウのハンドルは
最大または最小にされた
動作コードであり、
動作コードはウインドウ
が最大か、最小かまたは
再生されたかを示す
HCBT_CREATEWND
新しく生成された
ウインドウのハンドル
HOOKS
DLL
24
(Posted)
WH_HCBT_ACTIVATE
ウインドウのハンドルは
活性化されている
(Sent)
WH_HCBT_DESTROYWND
ウインドウのハンドルは
破壊されている
(Posted)
WH_HCBT_CBTMINMAX
ウインドウのハンドルは
変更されている
(Posted)
WS_HCBT_CREATEWND
ウインドウのハンドルは
生成されている
SW_HIDE
SW_SHOWMINIMIZED
SW_MINIMIZE
SW_RESTORE
SW_MAXIMIZE
SW_NORMAL
SW_SHOW
ＲＩＴＡ
主ウインドウ
23

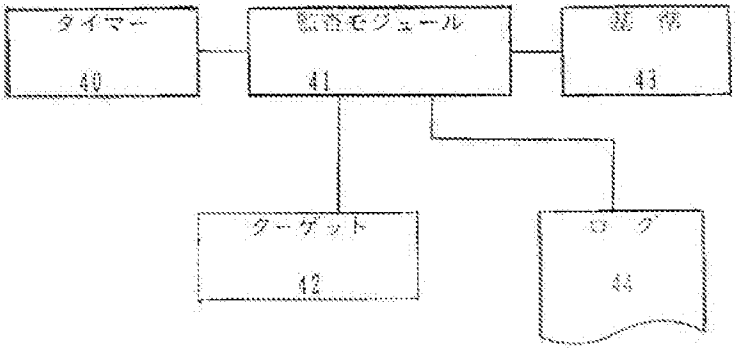
Ｆｉｇｕｒｅ３

【図４】



Ｆｉｇｕｒｅ４

【図５】



Ｆｉｇｕｒｅ５

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/10091

A. CLASSIFICATION OF SUBJECT MATTER
(IPC(6) :H04Q 9/02
US CL. :364/222.2, 222.5, 940.1; 395/600
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 364/222.2, 222.5, 222.81, 940.1; 395/600

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US, A, 5,032,979 (HECHT ET AL.) 16 July 1991, abstract and col. 11.	1-12 and 16-18
X	US, A, 5,406,269 (BARAN) 11 April 1995, abstract and fig 1.	1-5 and 9-14
A	US, A, 4,827,508 (SHEAR) 02 May 1989, abstract.	1-25
A, P	US, A, 5,483,658 (GRUBE ET AL.) 09 January 1996, abstract.	1-25

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be part of particular relevance
"B" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 JULY 1996	18 SEP 1996
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer CRAIG STEVEN MILLER Telephone No. (703) 305-3800

Form PCT/ISA/210 (second sheet)(July 1992)*

フロントページの続き

(81)指定国 EP(AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG), AP(KE, LS, MW, SD, SZ, UG), UA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, US, UZ, VN

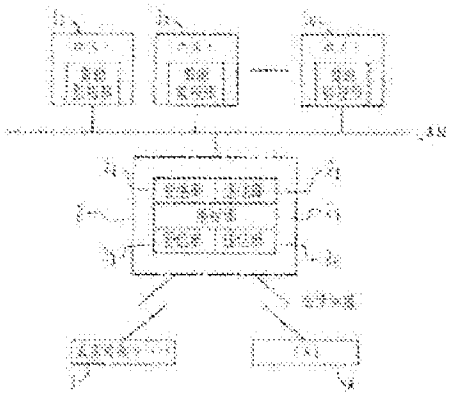
(72)発明者 ピンスレイ、 デイビッド・ビー
アメリカ合衆国、 ニューヨーク州 11021、グレート・ネック、パーストウ・ロード・5ディー 8
(72)発明者 ボロニウィッツ、 カレン・エー
アメリカ合衆国、 ニューヨーク州 11733、イースト・セトーケット、バッキンガム・メドウ・ロード 2
(72)発明者 コステロ、 スティーブン・ジェイ
アメリカ合衆国、 ニューヨーク州 11788、ホッポージ、ジョン・ストリート 122
(72)発明者 スタンジアーニ、スティーブン・エヌ
アメリカ合衆国、 ニューヨーク州 11803、プレインビュー、プローラル・アベニュー 236

ABNORMALITY MONITORING SYSTEM

Publication number: JP11003246 (A)
Publication date: 1999-01-06
Inventor(s): KARIYA MASATOSHI +
Applicant(s): MEIDENSHA ELECTRIC MFG CO LTD +
Classification:
- International: *G06F11/30;* (IPC1-7): G06F11/30
- European:
Application number: JP19970152749 19970611
Priority number(s): JP19970152749 19970611

Abstract of **JP 11003246 (A)**

PROBLEM TO BE SOLVED: To enable a system manager to accurately recognize the state of abnormality and to process the abnormality by using a function to estimate occurrence of the abnormality and also a function to collect and send the detailed error information based on the estimation of occurrence of the abnormality. SOLUTION: In an abnormality monitoring system, an abnormality processor 2 detects the abnormality of computers 11 to 1N respectively and sends the detected abnormality to the sending destination such as a system manager, etc., via a circuit. The processor 2 includes the sending parts 22 and 24 which send the information converted into the data to a LAN and the circuit, and an analysis part 25 which buffers the information transferred between the sending and receiving parts and analyzes the abnormality. Then the part 25 collects the error information from the computers 11 to 1N and sends these information to a prescribed sending destination. Furthermore, the part 25 analyzes the queue data received from each computer to estimate the occurrence of abnormality and then collects the detailed error information from each computer to send them to the prescribed sending destination.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開平11－3248
(43)公開日　平成11年(1999)１月６日

(51)Int.Cl.⁶	識別記号	Ｆ１	
Ｇ０６Ｆ　11/30		Ｇ０６Ｆ　11/30	Ｋ

審査請求　未請求　請求項の数１　ＯＬ　（全４頁）

(21)出願番号　特願平9－152749

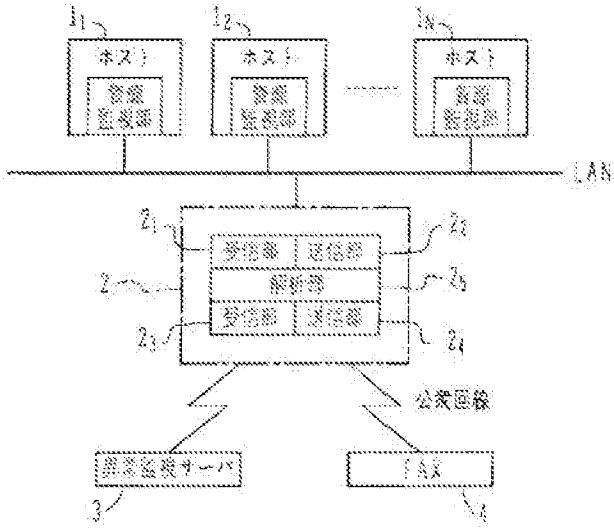
(22)出願日　平成９年(1997)６月11日

(71)出願人　000006105
株式会社明電舎
東京都品川区大崎２丁目１番17号
(72)発明者　苅谷　正年
東京都品川区大崎２丁目１番17号　株式会社明電舎内
(74)代理人　弁理士　志賀　富士弥　（外１名）

(54)【発明の名称】　異常監視方式

(57)【要約】
【課題】　各コンピュータがＬＡＮで接続されるコンピュータシステムに異常処理装置を接続し、この異常処理装置が各コンピュータからの異常情報をシステム管理者等に送信するのみでは、異常の分析や対応処理ができない。
【解決手段】　異常処理装置２は、ＬＡＮ及び公衆回線に対するデータ変換した情報の送信部2_2、2_4と受信部2_1、2_3及び送受信情報をデータベースにバッファリングして異常を解析する解析部2_5を備え、解析部は、各コンピュータ1_1～1_Nからのエラー情報を収集して予め定めた異常監視サーバ３やシステム管理者のＦＡＸ４に送信する機能と、各コンピュータからのキューデータを解析して異常発生を予測し、この予測がなされたときに当該コンピュータから詳細エラー情報を収集して予め定めた送信先に送信する機能とを備える。

システム構成図



1

【特許請求の範囲】

【請求項１】　各コンピュータがＬＡＮで接続されるコンピュータシステムに異常処理装置を接続し、この異常処理装置が各コンピュータの異常を検出してシステム管理者等の送信先に回線を通して送信する異常監視方式において、

前記異常処理装置は、ＬＡＮ及び回線に対するデータ変換した情報の送信部と受信部、及びこれら送信部と受信部による送受信情報をデータベースにバッファリングして異常を解析する解析部を備え、

前記解析部は、各コンピュータからのエラー情報を収集して予め定めた前記送信先に送信する機能と、各コンピュータからのキューデータを解析して異常発生を予測し、この予測がなされたときに当該コンピュータから詳細エラー情報を収集して予め定めた送信先に送信する機能とを備えたことを特徴とする異常監視方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＬＡＮ（ローカルエリアネットワーク）で接続されるコンピュータシステムにおける異常監視方式に関する。

【０００２】

【従来の技術】プラント等の監視制御システムは、ＬＡＮで接続されるコンピュータシステムを構築しており、プロセスコントローラによる現場機器の監視制御と、これらにＬＡＮで接続されるホストコンピュータによる監視やその監視制御を可能にする。

【０００３】この監視制御システムにおいて、コンピュータの異常監視には、各コンピュータでの異常発生を検出してシステム管理者に通報する異常処理装置がＬＡＮに接続されている。

【０００４】この異常処理装置は、異常検出部と異常通知部で構成され、異常検出部では主にコンピュータのハードウェアの異常信号からシステムのハードウェアの異常を監視し、異常通知部では専用回線又は公衆回線を利用して予め登録されている連絡先に対して音声又は規定的に異常を通知する。

【０００５】

【発明が解決しようとする課題】従来の異常処理装置による異常監視方式は、異常発生の有無をシステム管理者に通知するのみであり、異常状況等の詳細な情報を通知する機能を持たないし、異常発生に対する処理機能を持たない。

【０００６】このため、システム管理者は、ある資源に異常が発生したことを認識できるが、どのような異常発生かを認識できないし、異常発生に対する適切で迅速な処理操作を行うのが難しい。

【０００７】本発明の目的は、異常発生時にシステム管理者が異常状況の適確な認識及び異常処理ができる異常監視方式を提供することにある。

2

【０００８】

【課題を解決するための手段】本発明は、異常処理装置に異常の受動的な検出機能に加えてキューデータの能動的な収集により異常発生を予測する機能と、異常発生の予測で詳細なエラー情報を収集して送信する機能とを持たせるようにしたもので、以下の方式を特徴とする。

【０００９】各コンピュータがＬＡＮで接続されるコンピュータシステムに異常処理装置を接続し、この異常処理装置が各コンピュータの異常を検出してシステム管理者等の送信先に回線を通して送信する異常監視方式において、前記異常処理装置は、ＬＡＮ及び回線に対するデータ変換した情報の送信部と受信部、及びこれら送信部と受信部による送受信情報をデータベースにバッファリングして異常を解析する解析部を備え、前記解析部は、各コンピュータからのエラー情報を収集して予め定めた前記送信先に送信する機能と、各コンピュータからのキューデータを解析して異常発生を予測し、この予測がなされたときに当該コンピュータから詳細エラー情報を収集して予め定めた送信先に送信する機能とを備えたことを特徴とする。

【００１０】

【発明の実施の形態】図１は、本発明の実施形態を示す異常監視システムである。ローカルホスト群になる各コンピュータ1_1～1_nはＬＡＮで互いに接続され、このＬＡＮに異常処理装置２が接続される。

【００１１】異常処理装置２は、ＬＡＮを通して各コンピュータ1_1～1_nとの通信機能を持ち、さらに、公衆回線を通して異常処理装置の上位になる異常監視サーバ３やシステム管理者のファクシミリ（ＦＡＸ）に対する通信機能を持つ。

【００１２】異常処理装置２の受信部2_1及び送信部2_7は、ＬＡＮを通してコンピュータ1_1～1_nからのデータ変換機能を有して資源情報の受信及び異常発生時のエラー情報の要求出力等を行う。同様に、受信部2_3及び送信部2_4は、公衆回線で遠隔地に接続されたサーバ３等とのデータ送受信を行う。

【００１３】異常処理装置２の解析部2_5は、異常発生時にコンピュータ1_1～1_nからの受信データを分析し、その結果により対応を判断し、システム内の監視対象への制御指令や公衆回線により接続された機器へのデータ送信を決める。

【００１４】このような構成になる異常処理装置２により、監視対象コンピュータから異常通知先へのデータ変換と送信にとどまらず、解析部2_5を持つことで異常状況に能動的に対応することが可能となる。

【００１５】異常処理装置２による機能関連図を図２に示す。異常通知は、一般に受信部2_1→解析部2_5→送信部2_4の経路で行われる。受信部2_1と解析部2_5の間のデータ授受は、データベース2_6を介することにより、データのバッファリングを可能にする。また、解析部２

5から送信部2₂へのデータ収集要求を出すことで、より詳細な情報を収集できる。

【0016】送信部2₄では、登録された通知先に合わせてデータ変換し、その結果を送信する。

【0017】公衆回線上に接続された異常監視サーバがある場合には、受信部2₃→解析部2₅→送信部2₂を経由して情報収集あるいは障害復旧の制御指令を出力する。

【0018】図3は、異常処理装置2の解析部2₅の処理フローを示す。同図の（a）に示すエラー情報解析処理は、エラー信号が発生したときに異常を検知し、登録先に通知する受動的処理になる。具体的には、データベース2₆に異常データが収集されたとき（S1）、この異常データの分析により送信先（登録先）を検出し（S2）、すべての送信先に異常データを送信する（S3～S5））。

【0019】同図の（b）に示すキューデータ解析処理は、定期的な収集情報から能動的に異常を予測すると共に、異常と判断したときには必要に応じたエラー情報要求を出力する。具体的には、コンピュータのうち、キューデータの使用情報があり（S11）、一定値以上の資源を使用し（S12）、一定時間以上に資源を占有しているとき（S13）、当該コンピュータに詳細エラー情報の要求を出力し（S14）、この情報の分析により送信先の検出（S15）でデータを送信する（S16～S18）。

【0020】なお、各コンピュータの資源の使用量と占有時間は、システムの規模や負荷設定に応じて任意に設定され、この組み合わせを予め決定し、その値を変更することで監視レベルを設定可能にする。

【0021】

【発明の効果】以上のとおり、本発明によれば、異常処理装置に異常の受動的な検出機能に加えてキューデータの能動的な収集により異常発生を予測する機能と、異常発生の予測で詳細なエラー情報を収集して送信する機能とを持たせるようにしたため、以下の効果がある。

【0022】（1）異常の能動的な予測と詳細データ収集により、異常発生時にシステム管理者が異常状況の適確な認識及び異常発生に対する適確な処理ができる。

【0023】（2）異常情報の分析により送信先を決定するため、適確な情報送信ができる。

【0024】（3）異常の予測にレベル設定可能とすることにより段階的なエラー予測が可能となり、また監視対象機器等への制御も可能となる。

【0025】（4）受信情報をデータベースにバッファリングすることにより、解析部では送信先毎のデータフォーマットを考慮することなく送信処理できる。また、送信部でデータ変換及び送信処理するため、異常通知先の変更が容易となる。

【0026】（5）異常処理装置の上位に異常処理サーバを設けることにより、より詳細的に障害復旧が可能となる。また、データを蓄積することで障害発生プロセスを解析することが可能となる。

【図面の簡単な説明】

【図1】本発明の実施形態を示すシステム構成図。

【図2】実施形態における異常処理装置の機能関連図。

【図3】実施形態における解析部の処理フロー。

【符号の説明】

1₁～1ₙ…コンピュータ

2…異常処理装置

2₁、2₃…受信部

2₂、2₄…送信部

2₅…解析部

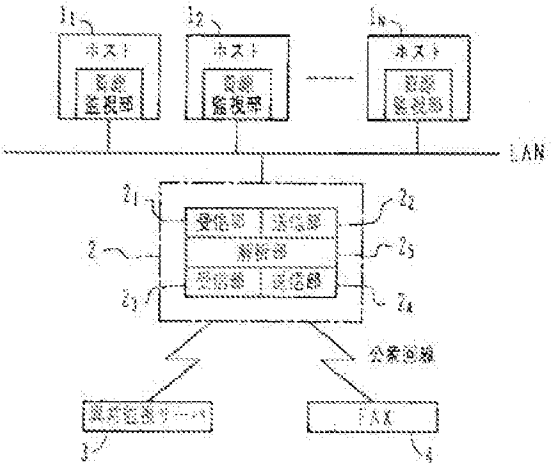
2₆…データベース

3…異常監視サーバ

4…ファクシミリ

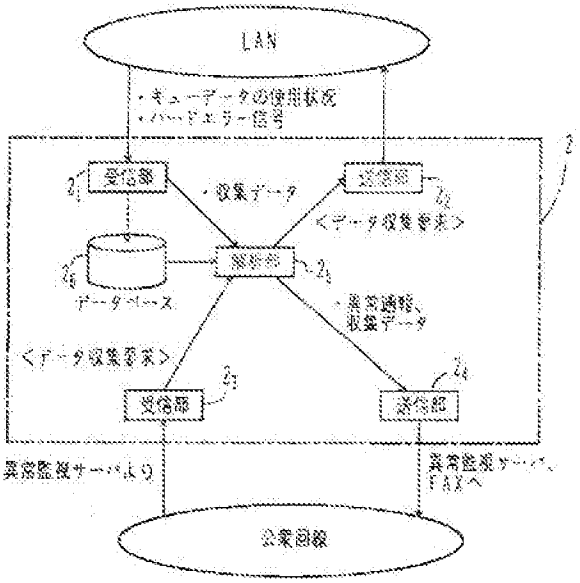
【図1】

システム構成図



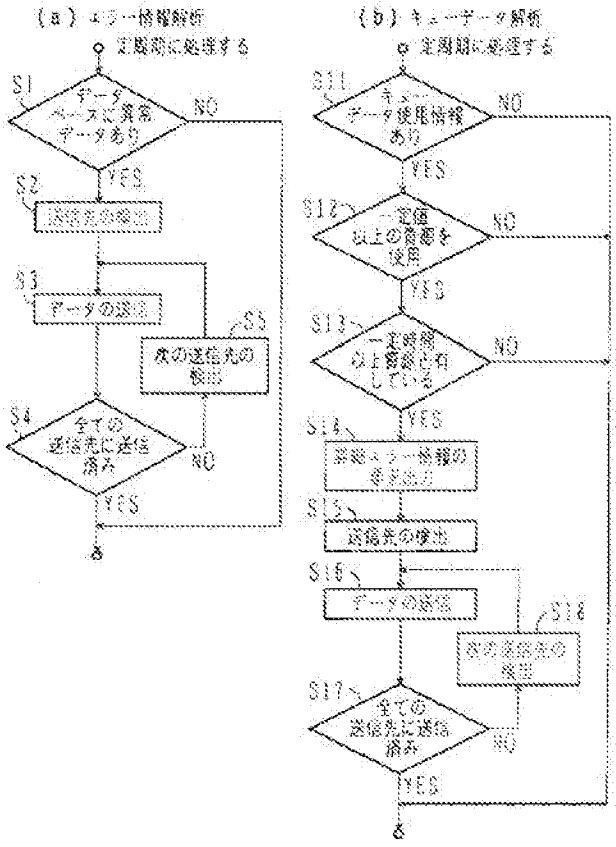
【図2】

機能関連図



【図3】

解析部の処理フロー

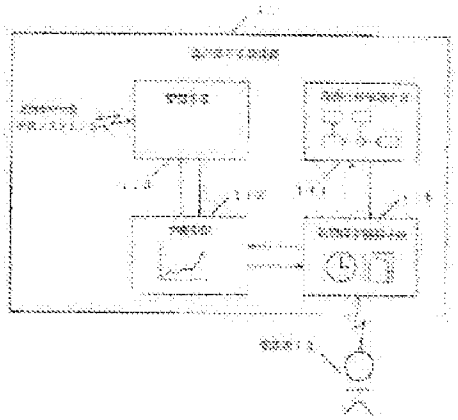


DECENTRALIZED SYSTEM OPERATION MAINTENANCE SUPPORT DEVICE AND OPERATION MAINTENANCE SUPPORTING METHOD

Publication number: JP10083382 (A)
Publication date: 1998-03-31
Inventor(s): NOZAWA YUKITERU +
Applicant(s): TOSHIBA CORP +
Classification:
- international: ***G06F11/30; G06F15/00; G06F15/16; G06F15/177; G06F9/46;*** (IPC1-7): G06F11/30; G06F15/00; G06F15/16; G06F9/46
- European:
Application number: JP19960237721 19960909
Priority number(s): JP19960237721 19960909

Abstract of **JP 10083382 (A)**

PROBLEM TO BE SOLVED: To maintain the operation of a decentralized system effectively, economically, and deliberately by controlling a total flow for advancing operation maintenance support by an operation maintenance control means. SOLUTION: The operation maintenance control means 110 controls a series of operations for operation maintenance support by receiving a distinctive operation maintenance support request from an administrator 13 or an internal synchronism generation. Further, a work specification managing means 111 manages the correspondence relation between application which embodies a work and the decentralized system mounted with it as specifications and provides necessary information in response to an inquiry from the operation maintenance control means 110. Further, a predicting means 112 predicts a future tendency of a constituent element of the decentralized system which is indicated by the operation maintenance control means 110 and considered to need to be maintained. Then a monitor means 113 operates as a dataware house for a monitor means in the operation-maintained decentralized system 10.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－83382

(43)公開日　平成10年(1998)３月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｇ０６Ｆ	15/16	４５０		Ｇ０６Ｆ	15/16	４５０Ｚ
	9/46	３６０			9/46	３６０Ｃ
	11/30				11/30	Ｅ
	15/00	３２０			15/00	３２０Ａ

審査請求　未請求　請求項の数８　ＯＬ　（全 21 頁）

(21)出願番号　特願平8－237721

(22)出願日　平成８年(1996)９月９日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　野澤　幸輝
東京都府中市東芝町１番地　株式会社東芝府中工場内

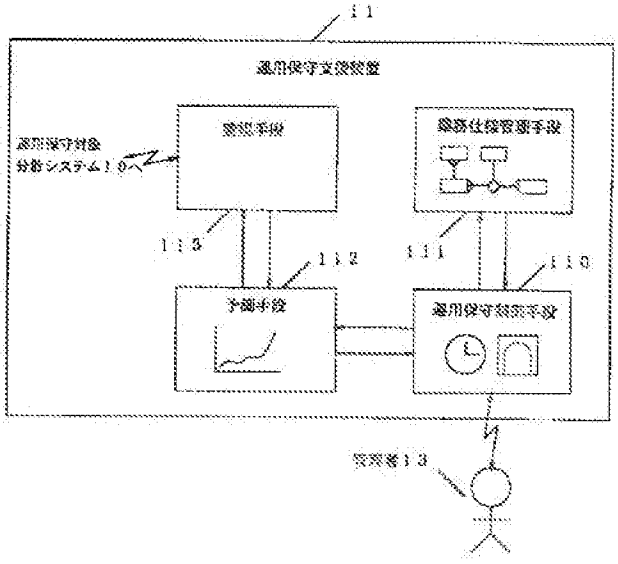
(74)代理人　弁理士　木内　光春

(54)【発明の名称】　分散システム運用保守支援装置および運用保守支援方法

(57)【要約】

【課題】　分散システムの運用保守を効果的、経済的かつ計画的に行えるようにした分散システム運用保守支援装置および運用保守支援方法を提供する。

【解決手段】　本発明に係る分散システム運用保守支援装置１１は、運用保守支援を開始し、さらにその後に続く運用保守支援の一連の動作を制御する運用保守制御手段１１０と、業務を体現するアプリケーションとそれが実装される分散システムとの間の対応関係を所定の仕様として管理し、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理手段１１１と、運用保守が必要な分散システムの構成要素に対して、将来的な動向を予測する予測手段１１２と、分散システムから収集した運用保守情報を予測手段に伝える監視手段１１３とから構成されている。



1

【特許請求の範囲】

【請求項１】　複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援装置であって、

前記分散システムの運用保守支援を開始し、さらにその後に続く運用保守支援動作を制御する運用保守制御手段と、

前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御手段からの問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理手段と、

前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視手段とを備えたことを特徴とする分散システム運用保守支援装置。

【請求項２】　複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援装置であって、

前記分散システムの運用保守支援を開始し、さらにその後に続く運用保守支援動作を制御する運用保守制御手段と、

前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御手段からの問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理手段と、

前記分散システムの構成要素の内、運用保守制御手段により指示された構成要素の将来的な動向を予測する予測手段と、

前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視手段とを備えたことを特徴とする分散システム運用保守支援装置。

【請求項３】　前記予測手段が、前記監視手段によって収集された運用保守情報と、予測に当てはめられる予測モデルとに基づいて、分散システムの構成要素の将来的な動向を予測するように構成されていることを特徴とする請求項２に記載の分散システム運用保守支援装置。

【請求項４】　前記運用保守制御手段が、運用保守対象とすべき業務の重要度を自動的に設定するように構成されていることを特徴とする請求項１乃至請求項３のいずれか一に記載の分散システム運用保守支援装置。

【請求項５】　複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援方法であって、

前記分散システムの運用保守支援を開始し、さらにその後に続く運用保守支援動作を制御する運用保守制御ステップと、

前記分散システムの構成要素とその分散システムに実装

2

される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御ステップにおける問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理ステップと、

前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視ステップとを含むことを特徴とする分散システム運用保守支援方法。

【請求項６】　複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援方法であって、

前記分散システムの運用保守支援を開始し、さらにその後に続く運用保守支援動作を制御する運用保守制御ステップと、

前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御ステップにおける問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理ステップと、

前記分散システムの構成要素の内、運用保守制御ステップにおいて指示された構成要素の将来的な動向を予測する予測ステップと、

前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視ステップとを含むことを特徴とする分散システム運用保守支援方法。

【請求項７】　前記予測ステップが、前記監視ステップによって収集された運用保守情報と、予測に当てはめられる予測モデルとに基づいて、分散システムの構成要素の将来的な動向を予測するように構成されていることを特徴とする請求項６に記載の分散システム運用保守支援方法。

【請求項８】　前記運用保守制御ステップが、運用保守対象とすべき業務の重要度を自動的に設定するように構成されていることを特徴とする請求項５乃至請求項７のいずれか一に記載の分散システム運用保守支援方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数の計算機およびその周辺機器をネットワークを介して構成した分散システムの運用保守を支援するための分散システム運用保守支援装置および運用保守支援方法に関する。

【０００２】

【従来の技術】従来、複数の計算機およびその周辺機器をネットワークを介して構成した分散システム（以下、分散システムと総称する）については、いかにして分散システムの処理性能を上げるか、あるいは信頼性を上げるかといった観点からの研究開発に重点が置かれていた。しかし、この分散システムをどのように運用保守していくべきかという点も非常に重要である。

3

【０００３】ここで、上記「分散システムの運用保守」とは、「分散システムの利用者であるエンドユーザが、分散システム上に実装された業務アプリケーションを、十分有効に、かつ支障なく利用できるようにするために、分散システムの管理者が、既にサービスの提供を実施している分散システムの構成要素を適切に維持していくこと」と定義される。

【０００４】たとえば、ある業務において重要な役割を担うサーバがある場合、当サーバが十分なパフォーマンスを発揮しつづけられるように、当サーバのディスクやメモリ、あるいは当サーバに関係するネットワークなどのシステムリソースを、必要に応じて強化していくといった、ハードウェアに対する作業が挙げられる。また、別の例としては、ある業務に関連したトランザクションを構成するプロセスについて、その実行をクライアント側からサーバ側へ移すといった、ソフトウェアに対する作業が挙げられる。

【０００５】このような分散システムの運用保守に関する技術としては、例えば、特開平６－１４９７３７号公報に示された発明がある。この発明は、負荷分散による処理性能の向上や、危険分散による信頼性の向上、あるいはいわゆるダウンサイジングによるコストの抑制など、分散システムの利点を活かしつつ、集中管理方式を導入することで、分散システムの運用保守を容易にすることを目的としている。

【０００６】また、前記集中管理方式の導入にあたっては、まず、島と呼ばれる任意数の計算機およびその周辺機器からなる管理単位を設定し、この島毎にコントロールサーバと呼ばれる管理システムを割り当てる。さらに、任意数の島を一括して管理するために、マスターサーバと呼ばれる管理システムを割り当てる。

【０００７】このように構成することによって、マスターサーバによる集中的／一元的な運用保守が可能となり、マスターサーバの過負荷が問題になるような場合でも、ある島に特有の運用保守は、その島に割り当てられているコントロールサーバに任せることで、マスターサーバの過負荷を防ぐことを可能としている。また、このような集中管理方式を採用することによる効果として、ユーザ管理、アカウント管理、プログラム配布、ネットワーク構成管理、ネットワーク状況監視、障害対応、周辺機器の管理などを、効果的かつ容易に行うことができるとしている。

【０００８】しかし、分散システムの運用保守にあたって、前記発明によっても解決されない課題がいくつか存在する。すなわち、前記発明においては、分散システムを、その上に実装されている業務アプリケーションの持つ「意味」とは無関係に運用保守しているので、業務上重要と思われる管理対象と、さほど重要と思われない管理対象とが、同レベルで等しく管理されることになる。その結果、分散システムのエンドユーザが「もっとも重要である」と考えている業務に関連した運用保守対象が優先して運用保守されないという問題が生じていた。また、すべての管理対象が同レベルで管理されるため、運用保守にかかるコストに無駄が生じるといった問題も生じていた。

4

【０００９】例えば、前記発明に示されているサーバの障害検知の実施例についてみると、前記発明においては、分散システムのエンドユーザがもっとも重要であると考えている業務のためのサービスを、どのサーバが請け負っているのかについて把握することができないため、エンドユーザにとって重要度の高い業務に関連したサーバが優先して運用保守されなかった。また、分散システムの管理者は、分散システムに含まれるすべてのサーバについて、一様なコストをかけて管理しなければならず、分散システムの運用保守にかかるコストに無駄が生じていた。

【００１０】さらに、前記発明においては、分散システム内で発生した障害などについての運用保守上必要な情報は、それらの障害などが起こったあとに初めて分散システムの管理者によって把握されるので、運用保守が常に後手にまわってしまうという問題が生じていた。その結果、分散システムのエンドユーザは、分散システム内で発生した障害などによって、本来受けられるべきサービスが突然受けられなくなったり、あるいは非常に低い処理性能のもとでしかサービスを受けられなくなったりするなど、本来の品質を保ったサービスを受けることができず、多大な不利益を被る危険性が高かった。

【００１１】すなわち、前記発明によって得られる運用保守装置においては、各サーバのディスク使用量などの情報を監視できることが示されているものの、その情報をどのように扱うかについての詳細が記述されておらず、上述したような運用保守が後手にまわってしまうという問題を解決できていない。

【００１２】次に、分散システムの運用保守に関する他の技術としては、例えば、特開平７－２１０５５９号公報に示された発明がある。この発明は、分散システム内で発生する障害などについての情報を、一括して採取／収集／編集／転送できるような集中管理方式を導入することで、分散システムの構成要素単位ではなく、分散システム全体にわたる運用保守を可能にすることを目的としている。

【００１３】また、前記集中管理方式の導入にあたっては、上述した特開平６－１４９７３７号公報に示された発明とほぼ同じく、最上位の統合サーバ、営業所毎の対象サーバ、そしてクライアントからなる階層を構成し、運用保守上必要な情報が下位の階層から上位の階層に転送されていくようにすることで、集中管理を可能としている。さらに、この発明においては、運用保守上必要な情報の形式および内容を、オブジェクト指向の考え方に基づいて規定することを提案している。これによ

5

り、運用保守上必要な情報を、特定のソフトウェアなどの環境に依存しない形で管理することができるようにしている。

【0014】しかし、分散システムの運用保守にあたって、前記発明によっても解決されない課題がいくつか存在する。すなわち、業務毎に異なる特性が意識されないことに起因して、重点を置くべき運用保守対象が優先されて処理されず、また、すべての運用保守対象を同レベルで扱うため、無駄なコストが発生するという点である。すなわち、この発明においても、業務アプリケーションの「意味」と分散システムとを関連付ける技術についてはなんら示されておらず、結果として、優先的に運用保守を行うべき対象を特定することができないまま、無駄な運用保守コストが発生している。

【0015】さらに、この発明においても、運用保守上必要な情報が管理者に伝わるのか、障害などが発生した後になってしまうので、運用保守が常に後手にまわってしまうという問題も生じていた。なお、この発明においては、「予防保守」という表現によって、運用保守が後手にまわってしまう課題を意識していることが表わされているが、定期的かつ定量的に分散システムの構成要素を管理すること以上の、具体的な運用保守の方法については言及されておらず、運用保守が後手にまわってしまう課題を解決できているとはいえない。

【0016】また、分散システムの運用保守の観点に基づく他の技術としては、米国Ｈｅｗｌｅｔｔ－Ｐａｃｋａｒｄ社の、ＨＰ　ＯｐｅｎＶｉｅｗという製品がある（日経データプロ・ソフト　１９９５年　２月号　ｐ．２５１－２６０）。この製品は大きくネットワーク管理製品群とシステム管理製品群に分かれている。ネットワーク管理製品群の中核となるのは、ＨＰ　ＯｐｅｎＶｉｅｗ　ネットワーク・ノード・マネージャと呼ばれる製品であり、ＳＮＭＰ（Ｓｉｍｐｌｅ　Ｎｅｔｗｏｒｋ　Ｍａｎａｇｅｍｅｎｔ　Ｐｒｏｔｏｃｏｌ）ベースで、ネットワークについての障害管理、構成管理、性能管理を行う。また、システム管理製品群の中核となるのは、ＨＰ　ＯｐｅｎＶｉｅｗ　Ｏｐｅｒａｔｉｏｎｓ　Ｃｅｎｔｅｒと呼ばれる製品であり、ＳＮＭＰベースで、システムについてのイベント管理、ソフトウェア配布、ファイル等のバックアップ、負荷状況の把握などを行う。

【0017】しかし、この製品によっても先に示した運用保守上の課題は解決されない。すなわち、この製品においても、分散システム上に実装されている業務アプリケーションの「意味」と分散システムとを明示的に関連付ける手段は提供されておらず、重点を置くべき運用保守対象が優先されて処理されず、また、すべての運用保守対象を同レベルで扱うため、無駄なコストが発生するという問題が生じている。

【0018】確かに、ネットワーク管理のサブ製品であるＨＰ　ＯｐｅｎＶｉｅｗ　Ｈｉｓｔｏｒｙ　Ａｎａ

6

ｌｙｚｅｒ　では、特定のサービスを多く利用しているユーザの状況を把握でき、このことによって一部の局面では、業務の「意味」と分散システムの関連付けはなされているということができるが、業務のもつ重要性は、ユーザのサービス利用数とは直接相関関係にあるとはいえない。例えば、非常に重要な基幹業務などは、ごく限られたユーザがごく限られたタイミングでしかサービスを受けないものと考えられるからである。

【0019】さらに、この製品においては、システム管理のサブ製品であるＨＰ　Ｐｅｒｆ－ＩＲＸ　およびＨＰ　ＰＣＳ　と呼ばれる製品によって、分散システムの構成要素に対しての性能管理データの収集および将来動向予測などのデータ分析を可能にしている。しかし、業務の特性を意識した、重点をおくべき運用保守対象を特定できていないため、データ分析を適切に行えず、結果として適切でない分析結果による運用保守が行われてしまう危険性があった。

【0020】

【発明が解決しようとする課題】上述したように、従来の分散システムの運用保守支援技術は、どの業務が重要であるかといった業務のもつ「意味」と、分散システムの構成要素を適切に関連付けるための十分な手段を提供しておらず、また、分散システムに対する適切な分析手段を提供しないまま、運用保守を支援していた。

【0021】その結果、解決すべき課題として次の3点が挙げられる。すなわち、（1）分散システムのエンドユーザがもっとも重要であると考えている業務に関連した運用保守対象が、優先して運用保守されない。（2）重要でない業務に関連した運用保守対象も、すべて平等に運用保守されてしまい、運用保守コストに無駄が発生してしまう。（3）運用保守対象を特定するための分析が適切に行えず、有効な運用保守計画を立案することができない。

【0022】本発明は、上述したような従来技術の問題点を解決するために提案されたもので、その目的は、分散システムの運用保守を効果的、経済的かつ計画的に行えるようにした分散システム運用保守支援装置および運用保守支援方法を提供することにある。

【0023】

【課題を解決するための手段】上記の目的を達成するために、請求項1に記載の発明は、複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援装置であって、前記分散システムの運用保守支援を開始し、さらにその後に続く運用保守支援動作を制御する運用保守制御手段と、前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御手段からの問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理手段と、前記分

7

散システムから、運用保守支援のために必要な運用保守情報を収集する監視手段とを備えたことを特徴とするものである。

【００２４】また、請求項５に記載の発明は、請求項１に記載の発明を方法の観点から捉えたものであり、複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援方法であって、前記分散システムの運用保守支援を開始し、さらにその後に続く運用保守支援動作を制御する運用保守制御ステップと、前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御ステップにおける問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理ステップと、前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視ステップとを含むことを特徴とするものである。

【００２５】このような構成を有する請求項１に記載の分散システム運用保守支援装置あるいは請求項５に記載の分散システム運用保守支援方法においては、運用保守支援を進める上での全体的な流れを、運用保守制御手段が制御する。この流れは、運用保守制御手段内に保持されている起動を司る仕組みによって開始され、それとともに分散システムのエンドユーザがもっとも重要であると考えている業務が何であるかについての情報とそれに付随する情報が取得される。この段階で、エンドユーザにとって優先されるべき運用保守が正しく実施されることが保証され、効果的な運用保守が可能となる。さらに、業務仕様管理手段によって、分散システムのエンドユーザがもっとも重要であると考えている業務と、運用保守が必要になるかも知れない分散システム内の構成要素が関連づけられる。この段階で、無駄な運用保守コストの発生を抑えることができるようになり、経済的な運用保守が可能となる。

【００２６】請求項２に記載の発明は、複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援装置であって、前記分散システムの運用保守支援を開始し、さらにその後に続く運用保守支援動作を制御する運用保守制御手段と、前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御手段からの問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理手段と、前記分散システムの構成要素の内、運用保守制御手段により指示された構成要素の将来的な動向を予測する予測手段と、前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視手段とを備えたことを特徴とするものである。

【００２７】また、請求項６に記載の発明は、請求項２

8

に記載の発明を方法の観点から捉えたものであり、複数の計算機およびその周辺機器をネットワークを介して構成した分散システムに対する運用保守支援方法であって、前記分散システムの運用保守支援を開始し、さらにその後に続く運用保守支援動作を制御する運用保守制御ステップと、前記分散システムの構成要素とその分散システムに実装される業務アプリケーションとの間の対応関係を所定の仕様として管理し、前記運用保守制御ステップにおける問い合わせに応じて、所定の業務情報及び所定の構成要素情報の少なくともいずれか一方を提供する業務仕様管理ステップと、前記分散システムの構成要素の内、運用保守制御ステップにおいて指示された構成要素の将来的な動向を予測する予測ステップと、前記分散システムから、運用保守支援のために必要な運用保守情報を収集する監視ステップとを含むことを特徴とするものである。

【００２８】このような構成を有する請求項２に記載の分散システム運用保守支援装置あるいは請求項６に記載の分散システム運用保守支援方法においては、請求項１あるいは請求項５に記載の発明と同様に、運用保守制御手段によって全体的な流れが制御され、業務仕様管理手段によって業務と分散システム内の構成要素が関連づられる。次に、予測手段において、運用保守が必要になるかも知れない分散システム内の構成要素の将来動向を予測し、運用保守が必要であることが判明した分散システム内の構成要素のみを特定する。この段階で、請求項１あるいは請求項５に記載した発明よりも、さらに無駄な運用保守コストの発生を抑えることができるようになり、より経済的な運用保守が可能となる。また、それと同時に、予測結果をもとにした適切な分析によって、有効な運用保守計画を立案することができるようになり、計画的な運用保守が可能となる。

【００２９】請求項３に記載の発明は、請求項２に記載の分散システム運用保守支援装置において、前記予測手段が、前記監視手段によって収集された運用保守情報と、予測に当てはめられる予測モデルとに基づいて、分散システムの構成要素の将来的な動向を予測するように構成されていることを特徴とするものである。

【００３０】また、請求項７に記載の発明は、請求項３に記載の発明を方法の観点から捉えたものであり、請求項６に記載の分散システム運用保守支援方法において、前記予測ステップが、前記監視ステップによって収集された運用保守情報と、予測に当てはめられる予測モデルとに基づいて、分散システムの構成要素の将来的な動向を予測するように構成されていることを特徴とするものである。

【００３１】このような構成を有する請求項３に記載の分散システム運用保守支援装置あるいは請求項７に記載の分散システム運用保守支援方法においては、適切な予測モデルから得られた予測結果をもとにして、適切な分

析を行うことができるので、有効な運用保守計画を立案することができるようになり、計画的な運用保守が可能となる。

【００３２】請求項４に記載の発明は、請求項１乃至請求項３のいずれか一に記載の分散システム運用保守支援装置において、前記運用保守制御手段が、運用保守対象とすべき業務の重要度を自動的に設定するように構成されていることを特徴とするものである。

【００３３】また、請求項８に記載の発明は、請求項４に記載の発明を方法の観点から捉えたものであり、請求項５乃至請求項７のいずれか一に記載の分散システム運用保守支援方法において、前記運用保守制御ステップが、運用保守対象とすべき業務の重要度を自動的に設定するように構成されていることを特徴とするものである。

【００３４】このような構成を有する請求項４に記載の分散システム運用保守支援装置あるいは請求項８に記載の分散システム運用保守支援方法においては、管理者が当初はあまり重要でないと考えていた業務を見逃す危険性を低く抑えることができるようになるので、より確実な運用保守を実施することが可能となる。

【００３５】

【発明の実施の形態】以下、本発明の実施形態について、図面を参照して具体的に説明する。

【００３６】［１．本発明による運用保守支援の全体像］図１は、本発明による運用保守支援の全体像を示したものである。すなわち、運用保守の対象となる分散システム（以下、運用保守対象分散システムと称する）１０は、エンドユーザ１２によって各種業務に利用され、また、本発明に係る運用保守支援装置１１によってその挙動が監視され、さらに、管理者１３によって運用保守される。一方、運用保守支援装置１１は、前記運用保守対象分散システム１０の挙動を監視し、管理者１３に対して運用保守支援を行う。また、エンドユーザ１２は、運用保守対象分散システム１０を業務に利用する上で、管理者１３に対して、どの業務が重要かといった業務の「意味」を要求として伝え、また、管理者１３から、運用保守対象分散システム１０をどのように運用保守するかについてアナウンスを受ける。さらに、管理者１３は、運用保守対象分散システム１０を運用保守支援装置１１の支援を受けながら運用保守し、また、エンドユーザ１２に運用保守対象分散システム１０をどのように運用保守するかについてアナウンスし、エンドユーザ１２からどの業務が重要かといった業務の「意味」を要求として受けとる。

【００３７】なお、前記運用保守対象分散システム１０と運用保守支援装置１１は、物理的に同じシステム上に実装されても、分けて実装されても良いし、さらには、一部混在する形で実装されても良い。論理上、運用保守対象分散システム１０と運用保守支援装置１１の間の区別がつけば良い。また、同様に、エンドユーザ１２と管理者１３が、実際には同一の個人、あるいは複数からなるグループでも構わない。

【００３８】［２．運用保守対象分散システムの構成］図２は、運用保守対象分散システム１０の詳細を示したものである。すなわち、運用保守対象分散システム１０は、複数の計算機１００（ＣＰＵ１０３あるいはメモリ１０４などを含む）、およびその周辺機器であるディスク１０５、ネットワーク１０６などから構成されている。ここで、前記計算機１００については、分散システムのアーキテクチャあるいはモデルによって、サーバ１０１やクライアント１０２といった区別を持たせることができる。なお周辺機器については、運用保守の必要性に応じてどのようなものを対象にするかが決まり、図２に示したディスク１０５に限定されるものではない。

【００３９】また、この運用保守対象分散システム１０には、本発明に係る運用保守支援装置１１と連携するための、分散システム内監視手段１０７が含まれている。この分散システム内監視手段１０７は、ＣＰＵ１０３やメモリ１０４、ディスク１０５、ネットワーク１０６などから、運用保守対象分散システムに必要な運用保守情報を収集する。すなわち、分散システム内監視手段１０７は、単にデータを収集する手段であり、既存の技術によって容易に構築できる部位である。例えば、従来の技術の項において挙げた ＨＰ　ＯｐｅｎＶｉｅｗ では、ＨＰ　ＯｐｅｎＶｉｅｗ　Ｔｒａｆｆｉｃ　Ｅｘｐｅｒｔ／ＥＸ という製品によって、ＬＡＮを流れるトラフィックを監視することができる。なお、分散システム内監視手段１０７が行う収集の方法などについては、本発明に係る運用保守支援装置１１から指示を受けて決定されるように構成されている。

【００４０】［３．運用保守支援装置の構成］図３は、本発明の対象である運用保守支援装置１１の構成を示したものである。すなわち、運用保守支援装置１１は、以下に詳述する運用保守制御手段１１０、業務仕様管理手段１１１、予測手段１１２、監視手段１１３とから構成されている。

【００４１】ここで、前記運用保守制御手段１１０は、管理者１３から明示的な運用保守支援依頼を受けるか、内部的な動機が発生することによって、運用保守支援を開始し、さらにその後に続く運用保守支援の一連の動作を制御するものである。また、前記業務仕様管理手段１１１は、業務を体現するアプリケーションと、それが実装される分散システムとの間の対応関係を仕様として管理しており、前記運用保守制御手段１１０からの問い合わせに応じて、必要な情報を提供するものである。さらに、前記予測手段１１２は、前記運用保守制御手段１１０から指示された、運用保守が必要と思われる分散システムの構成要素に対して、将来的な動向を予測するものである。また、監視手段１１３は、運用保守対象分散シ

11

ステム10内に含まれている前記分散システム内監視手段107に、データウェアハウスとしての側面を与える。すなわち、運用保守上必要なデータの収集の仕方に関して指示を与え、前記予測手段112が必要とする運用保守情報を収集させ、収集された運用保守情報を予測手段112に伝えるものである。

【0042】なお、運用保守対象分散システム10内の監視手段107は、単なるデータ収集の手段であったが、これに対して、運用保守支援装置11内の監視手段113は、分散システム内監視手段107から取り出したデータを、運用保守上利用しやすいような形式に変換するといった付加的な機能を有している。

【0043】〔2－1．運用保守制御手段の構成〕図4は、前記運用保守制御手段110の構成を示したものである。すなわち、運用保守制御手段110は、以下に詳述する窓口1100あるいはタイマ1101、またはその両方と、運用保守制御リスト1102、予測対象リスト1103、要求特性データ1104、予測データ1105、判断部1106および運用保守対象リスト1107とから構成されている。

【0044】（窓口）窓口1100は、管理者13が明示的／意識的に、運用保守対象分散システム10の運用保守支援を受けようと考えたときの窓口となる。すなわち、管理者13が、窓口1100から、どの業務について運用保守を行うかを入力することによって、運用保守制御手段110による制御が開始される。

【0045】ここで、図5は、窓口1100で行われる前記入力処理を受け付ける画面の一例を示したものである。すなわち、図5に示した例においては、「業務」と、その業務が投入される「ノード」が入力できるようになっている。また、ボタン20は、運用保守の必要があるかどうかが頻繁にチェックされる業務をまとめて指定できるボタンである。一方、運用保守の必要があるかどうかを個別にチェックしたい場合には、リストボックス21から所望の「業務」を個別に選んで指定することもできる。さらに、ボタン22は、ボタン20あるいはリストボックス21で選ばれた業務が通常投入されるノードをまとめて指定できるボタンである。一方、業務投入ノードを個別に指定したい場合には、リストボックス23から指定することもできる。なお、窓口1100から入力される情報、および窓口1100が提供するガイダンスは、必ずしも上記の通りでなくとも良い。

【0046】（タイマ）タイマ1101は、管理者13が明示的／意識的に運用保守を行おうとしない場合でも、運用保守支援装置11として自発的に運用保守支援を行うために必要とされるものである。すなわち、予めタイマ1101に設定された日時／時刻になると、運用保守制御手段110による制御が開始されるように構成されている。

【0047】（運用保守制御リスト）前記窓口1100

12

あるいはタイマ1101によって、運用保守制御手段110が起動されると、運用保守制御リスト1102に記述された内容にしたがって、どの業務を運用保守の対象とするかが決定される。

【0048】ここで、図6は、運用保守制御リスト1102の一例を示したものである。すなわち、窓口1100においてデフォルト業務が指定されたときには、受注業務と発注業務を対象とし、さらに窓口1100においてデフォルトノードが指定されたときには、東京と大阪を対象とすることが記述されている。また、図6の例では、タイマ1101によって起動される場合、毎月1日の午前3時と毎日午前5時に運用保守制御手段110を起動し、それぞれの場合に対象とすべき業務が何であるのかが記述されている。なお、運用保守制御リスト1102記述する内容および記述の方法は、必ずしも上記の通りでなくとも良い。

【0049】（予測対象リストおよび要求特性データ）運用保守制御手段110は、前記運用保守制御リスト1102の内容をもとに、業務仕様管理手段111に問い合わせを行い、業務に関連して運用保守の対象となり得る分散システムの構成要素（CPU103やメモリ104、ディスク105、ネットワーク106など）を記述した予測対象リスト1103、およびそれらの構成要素が満たすべき特性を要求として記述した要求特性データ1104を得る。

【0050】ここで、図7は、予測対象リスト1103の一例を示したものである。すなわち、図7の例では、予測を行うべき運用保守対象分散システム10内の構成要素として、“svr1”と名付けられているサーバのCPU、メモリ、ディスク、および“c111”、“c112”と名付けられているクライアントのCPU、メモリ、ディスク、および“svr1”と“c111”を結ぶネットワーク、および“svr1”と“c112”とを結ぶネットワークが指示されている。なお、予測対象リスト1103に記述する内容および記述の方法は、必ずしも上記の通りでなくとも良い。

【0051】また、図8は、要求特性データ1104の一例を示したものである。すなわち、図8の例では、予測を行うべき運用保守対象分散システム10内の構成要素が満たしていなければならない特性として、“svr1”と名付けられているサーバについて、そのCPUの最大負荷・平均負荷がどのようでなければならないか、およびメモリの最大ページフォールト数／平均ページフォールト数がどのようでなければならないか、およびディスクの余裕量がどのようでなければならないかといった情報が示されている。また、同様の内容が、“c111”、“c112”と名付けられているクライアントについても示されている。さらに、“svr1”と“c111”を結ぶネットワーク、および“svr1”と“c112”とを結ぶネットワークについて、それらの間を

流れる最大パケット数／平均パケット数がどのようでなければならないかが示されている。なお、この要求特性データ１１０４に載せられるデータは、後述する業務仕様管理手段１１１から得られるように構成されている。また、要求特性データ１１０４に記述する内容および記述の方法は、必ずしも上記の通りでなくとも良い。

【００５２】（予測データ）さらに、運用保守制御手段１１０は、予測対象リスト１１０３の内容を前記予測手段１１２に引き渡し、それぞれの分散システムの構成要素の予測動向を、予測データ１１０５として得る。この予測データ１１０５は、ある時系列なデータとして得られる。

【００５３】図９は、予測データ１１０５の一例を示したものである。すなわち、予測が行われた運用保守分散システム１０内の構成要素の予測動向として、一日単位で各構成要素がどのように推移するかが示されている。なお、予測データ１１０５に記述する内容、記述の方法および予測の時間間隔／期限などは、必ずしも上記の通りでなくとも良い。

【００５４】（判断部）さらに、運用保守制御手段１１０は、判断部１１０６において、運用保守制御リスト１１０２と要求特性データ１１０４と予測データ１１０５の内容を比較することにより、管理者１３に通告すべき運用保守対象リスト１１０７を作成する。

【００５５】ここで、前記判断部１１０６の動作について、図１０乃至図１２に示したフローチャートに基づいて説明する。まず、要求特性データ１１０４からデータを一つ取り出す（ステップ１００１）。例えば、図８に示した要求特性データ１１０４の例では、『"ｓｖｒ１"のＣＰＵについての平均負荷が０．１以下でなければならない』といったデータを取り出す。次に、予測データ１１０５のうち、現在に最も近い予測時点を選び（ステップ１００２）、予測データ１１０５から該当するデータを取り出す（ステップ１００３）。例えば、図９に示した予測データ１１０５の例では、現在に最も近い予測時点である明日（＝１ｄａｙ）を選ぶ。そして、その時点での予測値が、前記要求特性データ１１０４に示された要求値を越えているか否かを判定し（ステップ１００４）、越えている場合には、その構成要素を『問題あり』として記録する（ステップ１００５）。例えば、図９に示した予測データ１１０５の明日（＝１ｄａｙ）の例では、"ｓｖｒ１"のＣＰＵについての平均負荷は"０．１２"であり、図８に示された要求特性データ１１０４の要求値である"０．１"を越えているので、その旨記録する。そして、要求を越えていたことがわかった場合には、その時点をもってその構成要素の問題発生時点とし、それ以降については、その構成要素については調べない。

【００５６】一方、要求を越えていなければ次の予測時点に移り（ステップ１００６）、その予測時点における予測値が、前記要求特性データ１１０４に示された要求値を越えているか否かを判定し（ステップ１００４）、越えている場合には、その構成要素を『問題あり』として記録する（ステップ１００５）。そして、同様の処理を予測データが尽きるまで調べる（ステップ１００７）。例えば、図９に示した予測データ１１０５の場合には、問題が発見されない限り、１００日後（＝１００ｄａｙｓ）まで調べ続けられる。上記の処理を、要求特性データ１１０４に示されたすべてのデータについて繰り返す（ステップ１００８、ステップ１００９）。

【００５７】要求特性データ１１０４に示されたすべてのデータについて、上記の処理が終了した後、判断部１１０６においては、運用保守制御リスト１１０２から重要業務を一つ取り出す（ステップ１０１０）。例えば、図６に示した運用保守制御リスト１１０２の例では、重要業務として『受注業務』が選ばれる。さらに、事前の処理（ステップ１００１～ステップ１００９）による記録から、問題が発生する構成要素を一つ取り出す（ステップ１０１１）。例えば、先の例では、『"ｓｖｒ１"のＣＰＵ』が選ばれる。

【００５８】このとき、後述する業務仕様管理手段１１１に問い合わせて、重要業務がその構成要素を含んでいるか否かを判断する（ステップ１０１２）。そして、重要業務がその構成要素を含んでいる場合には、その構成要素に問題が発生する時点が、その重要業務を構成する他の構成要素に問題が発生する時点より早いか否かを調べ（ステップ１０１３）、それらのどれよりもより早い発生時点であれば、その構成要素を問題発生の原因とし、かつ、その発生時点を重要業務の問題発生時点とし（ステップ１０１４）、『どの重要業務に、いつ、何の問題が発生するか』を、運用保守対象リスト１１０７に載せる（ステップ１０１５）。例えば、先の例では、『重要業務として選ばれた『受注業務』が、『"ｓｖｒ１"のＣＰＵ』の平均負荷の増大により、明日には問題を引き起こす』といった内容が、運用保守対象リスト１１０７に記述される。

【００５９】また、原因に対する対策を示すことができる場合には、合わせてその対策も運用保守対象リスト１１０７に示される（ステップ１０１６、ステップ１０１７）。このような対策を示すためには、様々な方法が考えられるが、一つの方法としては、個々の構成要素毎に、それが原因となった場合の対策についての情報を持たせ、これを業務仕様管理手段１１１において直接管理させる方法が考えられる。また、判断部１１０６内に判断知識をルール化したものを置き、それを参照させる方法なども考えられる。

【００６０】以上の対応付けを、事前の処理（ステップ１００１～ステップ１００９）による記録のすべてについて繰り返す（ステップ１０１８、ステップ１０１９）。さらに、運用保守制御リスト１１０２に挙げられ

たすべての重要業務について、上記処理を繰り返す（ステップ１０２０、ステップ１０２１）。

【００６１】（運用保守対象リスト）次に、前記運用保守対象リスト１１０７について説明する。すなわち、図１３は、運用保守対象リスト１１０７の一例を示したものであるが、この例では、将来的に支障が出る業務とその日時および原因、さらに運用保守が必要な分散システム１０内の構成要素が指摘されており、これが管理者１３に通告されることになる。

【００６２】管理者１３は、この運用保守対象リスト１１０７を参照することによって、運用保守対象分散システム１０に問題が発生する前にそれを検知し、運用保守が必要な構成要素についてだけ、計画的に運用保守を実施することができるようになる。さらに、エンドユーザ１２は、運用保守対象リスト１１０７にしたがってなされる管理者１３からのアナウンスによって、突然十分なサービスを受けられなくなる状況を回避できるようになる。

【００６３】［３－２．運用保守制御手段における制御の流れ］図１４は、運用保守制御手段１１０における制御の流れを示したものである。すなわち、管理者１３が、窓口１１００から、どの業務について運用保守を行うかを入力することによって、運用保守制御手段１１０による制御が開始される（ステップ１４１）。あるいは、所定の日時／時刻を設定したタイマ１１０１によって、運用保守制御手段１１０による制御が自動的に開始される（ステップ１４２）。

【００６４】続いて、運用保守制御リスト１１０２に記述された内容にしたがって、どの業務を運用保守の対象とするかが決定され（ステップ１４３）、また、運用保守制御リスト１１０２の内容をもとに、業務仕様管理手段１１１に問い合わせることにより、運用保守の対象となり得る分散システムの構成要素を記述した予測対象リスト１１０３、およびそれらの構成要素が満たすべき特性を要求として記述した要求特性データ１１０４が得られる（ステップ１４４）。

【００６５】次に、予測手段１１２に予測を依頼することにより、それぞれの分散システムの構成要素の予測動向が、予測データ１１０５として得られる（ステップ１４５）。また、判断部１１０６において、運用保守制御リスト１１０２と要求特性データ１１０４と予測データ１１０５の内容が比較され（ステップ１４６）、運用保守対象リスト１１０７が作成されて、管理者１３に通告される（ステップ１４７）。

【００６６】［３－３．業務仕様管理手段の構成及び作用］図１５は、業務仕様管理手段１１１の構成を示したものである。すなわち、業務仕様管理手段１１１は、その内部に「業務」とその業務に関連した運用保守対象分散システム１０の構成要素との関係を保持したデータベース１１１０を保持している。また、このデータベース

１１１０では、業務１１１１、プロセス１１１２、テーブル１１１３、ノード１１１４、ＣＰＵ１１１５、メモリ１１１６、ディスク１１１７、ネットワーク１１１８の各構成要素と、各構成要素間の関係が管理されている。なお、図１５に示したデータベースにおいては、それぞれの関係をエンティティリレーションシップ図を用いて表している。また、ここでいう「ノード」とは、例えば、一つのＩＰアドレスを持つような計算機のことを意味している。

【００６７】次に、前記データベース１１１０をリレーショナルデータベースとして構築したときに、業務１１１１やプロセス１１１２などがどのように格納されるかについて、図１６～図２３を参照して説明する。

【００６８】すなわち、図１６には、「業務」について記述したテーブル（Ａ）と、業務に関連する「プロセス」を記述したテーブル（Ｂ）の２つが示されている。そして、この２つのテーブルから、「ある業務がどのようなプロセスから構築されているか」、また「その業務がどれだけの時間で処理を終えなければならないか」についての情報を得ることができる。

【００６９】また、図１７には、「プロセス」について記述したテーブル（Ａ）と、プロセスが配置されている「ノード」を記述したテーブル（Ｂ）と、プロセスが処理の対象とする「テーブル」およびその配置先を記述したテーブル（Ｃ）の３つが示されている。そして、この３つのテーブルから、「どのプロセスがどのノードで実行され」、「どのノードにあるどのテーブルにアクセスするか」、また「実行にあたって、どれだけの処理時間とメモリを消費するか」についての情報を得ることができる。なお、処理時間としては、仮定されたある処理性能を有する標準的な計算機によって処理が実行された場合に、必要とされる時間が表示されている。

【００７０】次に、図１８には、「テーブル」について記述したテーブル（Ａ）と、テーブルが配置されている「ノード」を記述したテーブル（Ｂ）の２つが示されている。また、図１９には、「ノード」について記述したテーブル（Ａ）と、ノードが保持しているＣＰＵ、メモリ、ディスク、ネットワークとの関連を記述したテーブル（Ｂ）～（Ｅ）の５つが示されている。さらに、図２０には「ＣＰＵ」について記述したテーブルが記述され、図２１には「メモリ」について記述したテーブルが記述されている。また、図２２には、「ディスク」について記述したテーブルが記述され、図２３には、「ネットワーク」について記述したテーブルが記述されている。

【００７１】そして、上記の図２０から図２３までに示された各テーブルの値は、図１６で示された業務１１１１のレスポンスタイムを満たすことができるように決定されている。例えば、受注業務（業務ＩＤ＝１００）のレスポンスタイムは３秒であることが要求されており

17

（図１６参照）、このとき受注業務によって使用される受注プロセス（プロセスＩＤ＝１０１）の処理時間が３００であり（図１７参照）、さらに、“ｓｖｒ１”のＣＰＵについてみると、その性能は標準として設定されたＣＰＵの２倍の性能であることから（図２０参照）、『“ｓｖｒ１”のＣＰＵがそれぞれ最大負荷が２、平均負荷が０．１を越えていては受注業務に要求されているレスポンスタイムを実現できない』といった判断を管理者１３が行うことで、値が決定される。

【００７２】なお、業務仕様管理手段１１１あるいはデータベース１１１０が管理する、上記図１６から図２３までに示されている構成要素の種類、管理方法については、必ずしも上記の通りでなくとも良い。

【００７３】［３－４．予測手段の構成及び作用］図２４は、予測手段１１２の構成を示したものである。すなわち、予測手段１１２は、その内部に、運用保守制御手段１１０から引き継いだ予測対象リスト１１０３と、各構成要素毎に適用される予測モデル１１２１、各構成要素毎の過去の推移リスト１１２０、各構成要素毎の予測データ１１２２、および運用保守制御手段１１０に引き渡す予測データ１１０５を保持している。

【００７４】ここで、各構成要素毎に適用される予測モデル１１２１は、予測を行いたい構成要素の過去の推移リスト１１２０と、他の構成要素の過去の推移リスト１１２０とを組み合わせて使用される。例えば、ＣＰＵの負荷予測を行うことを考えた場合、当然のことながらＣＰＵ自身の過去の推移も参照するべきであるし、また、メモリの影響を受けるのであれば、メモリについての過去の推移を参照しても良い。さらに予測モデル１１２１は、統計的な算術式によるものでも良いし、いわゆるニューラルネットワークモデルに基づくような自己学習型の予測手段をモデル化したものでも良い。

18

【００７５】そして、最終的に予測手段１１２は、各構成要素毎の予測データ１１２２を編集してまとめ、予測データ１１０５として運用保守制御手段１１０に引き渡すように構成されている。

【００７６】（統計的な手段を用いた予測モデルの一例）ここで、統計的な手段を用いた予測モデルの一例として、ディスク１０５の使用量の将来動向の予測を扱ってみる。なお、予測にあたっては、次の２つの前提を置く。すなわち、（１）ディスク１０５の使用量は、ユーザ数と強い相関関係にある。（２）ユーザ数は、時間と共に直線的に増加する。

【００７７】このような前提のもとでは、先にユーザ数の変化を予測し、それを基にディスク１０５の使用量の変化を予測することになる。まず、ある時刻x_iのもとでユーザ数がy_iであったとすると、前提（２）より、両者の関係は次のように表わされる。

【００７８】

【数１】$$y = ax + b \qquad \cdots (1)$$

上式における“ａ”および“ｂ”は、増加（あるいは減少）傾向を表すための係数である。この“ａ”および“ｂ”を最小２乗法によって求めるために、以下の連立方程式を解く。

【００７９】

【数２】

$$\begin{cases} a\sum_{i=1}^{n} x_i^2 + b\sum_{i=1}^{n} x_i = \sum_{i=1}^{n} x_i y_i \\ a\sum_{i=1}^{n} x_i + nb = \sum_{i=1}^{n} y_i \end{cases} \qquad \cdots\cdots (2)$$

すると、解は、以下のようになる。

【００８０】

※【数３】

$$\begin{cases} a = \dfrac{n\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sum_{i=1}^{n} y_i}{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2} \\ b = \dfrac{-\sum_{i=1}^{n} x_i \sum_{i=1}^{n} x_i y_i + \sum_{i=1}^{n} x_i^2 \sum_{i=1}^{n} y_i}{n\sum_{i=1}^{n} x_i^2 - \left(\sum_{i=1}^{n} x_i\right)^2} \end{cases} \qquad \cdots\cdots (3)$$

次に、以上によって求められたユーザ数y_iを基に、ディスク１０５の使用量z_iを求める。前提（１）より、両者の関係は以下のような回帰直線によって表わされる。なお、この回帰直線は、ｚのｙへの回帰直線とする。

【００８１】

【数４】

$$z = \frac{\sigma_z}{\sigma_y}\rho_{y,z}\,y + \bar{z} - \frac{\sigma_z}{\sigma_y}\rho_{y,z}\,\bar{y} \qquad \cdots\cdots (4)$$

上式において、σ_yはｙの標準偏差、σ_zはｚの標準偏

19

差，ρ_{yz}はｙとｚの相関係数を表し、ｙの平均値はｙの上にバーを付し、ｚの平均値はｚの上にバーを付して表している。

【００８２】以上に示した一連の式（１）から式（４）が予測モデルとして機能することによって、ディスク１０５の使用量の将来動向を予測することが可能となる。

【００８３】（自己学習的な手段を用いた予測モデルの一例）次に、自己学習的な手段を用いた予測モデルの一例として、ネットワーク１０６の負荷の将来動向の予測を扱ってみる。なお、ここでは自己学習型の予測手段として、図２５に示すような多層型ニューラルネットワーク３０を採用するものとする。また、予測にあたって、ネットワーク１０６の負荷は、自己の過去の推移から予測可能であるという前提を置く。さらに、このニューラルネットワーク３０を構成するニューロン３２は、図２６に示すようなシグモイド関数３１と呼ばれる非線型モデルによって表現されるものとする。

【００８４】まず、本予測手段１１２を含んだ運用保守支援装置１１の利用に先立って準備を行う。すなわち、ネットワーク１０６の負荷の過去の推移を教師値として、対応する入力層３３の値３４（＝ｘ）およびネットワークの重みに基づく出力層３７の値３８（＝ｚ）との誤差が最小になるように、ニューロン間の重み係数３０（＝ｗ）を更新しておく。

【００８５】なお、この学習のためには、バックプロパゲーション法が用いられる。また、予測を行うには、予測を行おうとする時点および、それより過去の時点のネットワーク１０６の負荷からなる値のリストｘ＝（x_1，x_2，x_3，．．．．．，x_n）を入力として、以下の式（５）から式（８）によってネットワークの出力値３８（＝ｚ）が求められる。

【００８６】

【数５】

$$g_j(x) = \sum_{i=1}^{n}(w_{ij}x_i) \qquad \text{------ (5)}$$

【数６】

$$y_j(x) = \frac{1}{1+\exp(-g_j(x))} \qquad \text{------- (6)}$$

【数７】

$$g(x) = \sum_{j=1}^{m}(w_j y_j(x)) \qquad \text{------- (7)}$$

【数８】

$$z(x) = \frac{1}{1+\exp(-g(x))} \qquad \text{------- (8)}$$

なお、入力値３４や中間値３６、あるいは出力値３８は、実際の値から正規化／逆正規化して扱う必要がある。すなわち、ネットワーク１０６の負荷の場合、実際に流れるパケットの量を表す数百や数千といった値を正規化して０近傍の値に変換してから入力値３４としたり、０から１の間までの値として出力された出力値も逆正規化して実際のパケット量を表すようにしてやる必要がある。この正規化／逆正規化は、ニューラルネットワークの汎化性を高めるという意味からも必要なものである。

20

【００８７】以上に示した多層型ニューラルネットワークが予測モデルとして機能することによって、ネットワーク１０６の負荷の将来動向を予測することが可能となる。また、このような自己学習型の予測モデルを採用することで、どの時間帯に業務が集中するかといった情報を明示的に示さなくても、それらの情報を考慮できるようになる。

【００８８】［４．本実施形態の運用保守支援装置の効果］上述したように、本実施形態の運用保守支援装置においては、この装置を構成する上記各手段によって、「どの業務を運用保守の対象とすべきか」、「その業務に関連する分散システム内の構成要素は何か」、「その構成要素が満たすべき特性はどのようなものか」、「その構成要素の将来的な動向はどのようなものか」といった観点で、分散システムの運用保守を支援する処理が進められる。

【００８９】その結果、重要な業務に関連した運用保守対象を優先して運用保守することができ、また、運用保守に対して優先度をつけることができるので、無駄な運用保守コストの発生を抑えることができる。さらに、運用保守を行うための分析が適切に行えるので、有効な運用保守計画を立てることができる。

【００９０】

【実施例】以下に、より具体的な実施例を用いて、運用保守が想定される幾つかの場面において、本発明が提案する運用保守支援装置および方法によって得られる作用・効果について説明する。

【００９１】まず始めの例として、Ｗｏｒｌｄ Ｗｉｄｅ Ｗｅｂを利用した情報提供を行うための分散システムを取り上げる。図２７は、この分散システムの概要を示したものである。すなわち、図２７において、分散システム５０では、ネットワーク５３に接続された多数のクライアント５２が、ＨＴＴＰ（Ｈｙｐｅｒ Ｔｅｘｔ Ｔｒａｎｓｆｅｒ Ｐｒｏｔｏｃｏｌ）サーバ５１ａおよび５１ｂへアクセスする。また、この分散システム５０のエンドユーザ５４は、この分散システム５０を利用して、情報検索を行うものとする。

【００９２】ここで、情報検索には２種類あり、随時頻繁に行われ、結果も数秒で返ってこなければならない検索処理５０ａと、不定期でそれほど頻繁でもなく、結果も翌日返ってくればよい検索処理５０ｂがあるものとする。なお、想定している状況では、クライアント５２の

台数が、なおも日に日に増加している最中であるとする。

【００９３】これまでの運用保守技術では、クライアント５２の台数の増加に伴って、分散システム５０内のすべての構成要素の増強を検討しなければならず、その結果、実施する運用保守も必ずしも適切なものであるという保証はなかった。

【００９４】しかしながら、本発明による運用保守技術では、管理者５５が運用保守支援装置から運用保守支援を受けることにより、業務の「意味」を考慮した適切な運用保守を行うことができるようになる。すなわち、上述した図１から図２４にしたがって説明すると、管理者５５が任意の時点で運用保守支援を受けるために窓口１１００を介するか、あるいはタイマ１１０１に設定された日時になるかのいずれかによって、運用保守支援装置１１が起動される。この運用保守支援装置１１内の運用保守制御手段１１０は、窓口１１００あるいは運用保守制御リスト１１０２から得られる情報（業務や、それに対する付随情報）により、運用保守の対象となる業務を特定し、業務仕様管理手段１１１に運用保守の必要があるかも知れない分散システム５０内の構成要素の選択を依頼する。

【００９５】続いて、業務仕様管理手段１１１は、指定された業務と、業務仕様管理手段１１１内で管理されているデータベース１１１０内の情報と照らし合わせることで、分散システム５０内において運用保守が必要になるかもしれない構成要素のみを選びだす。本例においては、重要な業務であると考えられる検索処理５０ａに関連した構成要素のみが選びだされ、検索処理５０ｂだけに関連した構成要素は選びだされない。

【００９６】この結果、運用保守制御手段１１０は、検索処理５０ａが行われるＨＴＴＰサーバ５１ａについて記載した予測対象リスト１１０３と、「検索処理５０ａは数秒で処理を終えなければならない」という要求特性データ１１０４を得る。さらに、運用保守制御手段１１０は、予測手段１１２に対して、ＨＴＴＰサーバ５１ａに関して、それに接続されるクライアント５２の増加に関連したＣＰＵやメモリ、あるいはディスク、ネットワークなどの構成要素の将来動向を、それぞれの過去の推移状況とモデルに照らし合わせて予測するよう依頼する。

【００９７】この予測の結果は、予測データ１１０５として運用保守制御手段１１０に渡され、判断部１１０６が運用保守制御リスト１１０２および要求特性データ１１０４と照らし合わせることで、運用保守上問題が発生する箇所とその時期を判断し、運用保守対象リスト１１０７としてまとめ、最終的に管理者５５に提示される。

【００９８】〔５．他の実施形態〕本発明は、上述した実施形態に限定されるものではなく、運用保守支援装置を運用保守制御手段１１０、業務仕様管理手段１１１及び監視手段１１３のみから構成することも可能である。なお、この場合は、分散システムのエンドユーザがもっとも重要であると考えている業務に関連した運用保守対象が優先して運用保守され、かつ、重要な業務に関連した運用保守対象が重点的に運用保守されることで、無駄な運用保守コストの発生を抑えることができる。

【００９９】また、前記運用保守制御手段１１０に設けられる窓口において、運用保守すべき業務の重要度を自動的に設定できるように構成することもできる。すなわち、図２８に示したように、窓口１１００には、保守指示履歴データベース１１０００と閾値１１００１が備えられている。なお、この保守指示履歴データベース１１０００は、窓口１１００から管理者１３が運用保守対象業務及び業務投入ノード等を明示するたびに、その業務が明示されたのは何回目か、あるいはその業務に対してそのノードが指定されたのは何回目なのかといった情報を格納するものである。また、閾値１１００１は、窓口１１００に予め設定されており、業務あるいは業務とノードの組み合わせについての保守指示回数がこの値を越えた場合には、運用保守制御リスト１１０２にその業務を重要業務として記載すべきか否かの検討が必要であるとの判断を下す基準となるものである。

【０１００】そして、この判断の結果、その保守指示回数が閾値１１００１を越えた業務を重要業務として自動的に運用保守制御リスト１１０２に追加しても良いし、図２９に示したように、ダイアログボックスなどのユーザインターフェースを提供することにより、管理者１３の了解を得たあとで運用保守制御リスト１１０２に追加しても良い。

【０１０１】このように構成することにより、管理者１３が当初はあまり重要でないと考えていた業務を見逃す危険性を低く抑えることができるようになる。なお、前記保守指示履歴データベース１１０００に格納する内容は、上述したものに限定されるものではなく、また、閾値１１００１についても、すべての業務あるいは業務とノードの組み合わせについて同じ値に設定しても、異なる値に設定しても良い。

【０１０２】

【発明の効果】以上説明したように本発明によれば、分散システム上に実装される業務の「意味」を意識することによって、分散システムのエンドユーザがもっとも重要であると考えている業務に関連した運用保守対象が優先して運用保守され、かつ、重要な業務に関連した運用保守対象が重点的に運用保守されることで、無駄な運用保守コストの発生を抑えることができ、かつ、運用保守を行うための分析が適切に行え、有効な運用保守計画を立てることができるようになる。

【図面の簡単な説明】

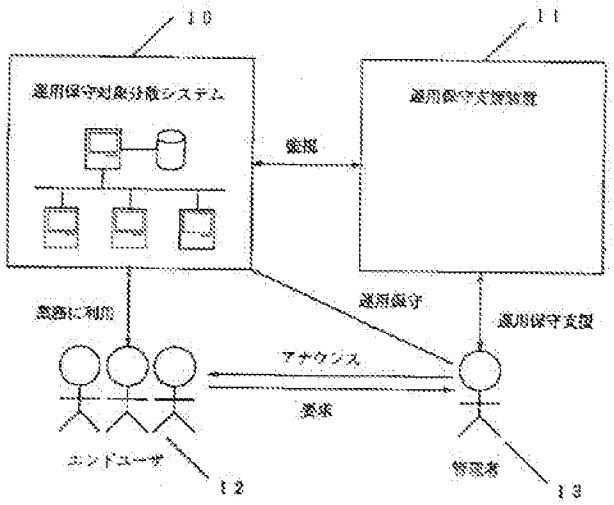
【図１】本発明による運用保守支援の全体像

【図２】運用保守対象分散システムの構成図

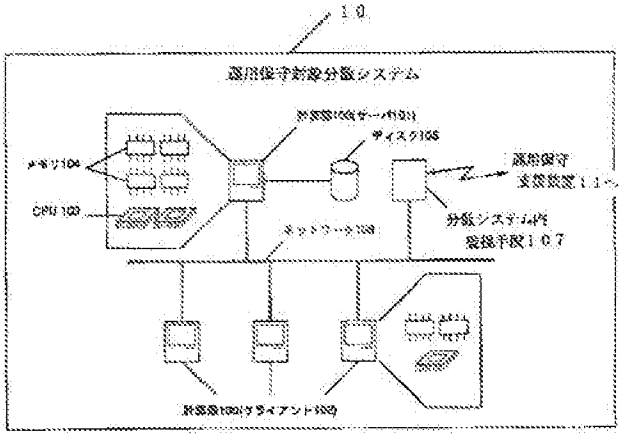
【図３】運用保守支援装置の構成図
【図４】運用保守制御手段の構成図
【図５】「窓口」で行われる入力処理を受け付ける画面の一例を示す図
【図６】運用保守制御リストの一例を示す図
【図７】予測対象リストの一例を示す図
【図８】要求特性データの一例を示す図
【図９】予測データの一例を示す図
【図１０】判断部における制御の流れの前段部を示すフローチャート
【図１１】判断部における制御の流れの中段部を示すフローチャート
【図１２】判断部における制御の流れの後段部を示すフローチャート
【図１３】運用保守対象リストの一例を示す図
【図１４】運用保守制御手段の制御の流れを示すフローチャート
【図１５】業務仕様管理手段の構成図

【図１６】業務の格納方法の一例を示す図
【図１７】プロセスの格納方法の一例を示す図
【図１８】テーブルの格納方法の一例を示す図
【図１９】ノードの格納方法の一例を示す図
【図２０】ＣＰＵの格納方法の一例を示す図
【図２１】メモリの格納方法の一例を示す図
【図２２】ディスクの格納方法の一例を示す図
【図２３】ネットワークの格納方法の一例を示す図
【図２４】予測手段の構成図
【図２５】多層型ニューラルネットワークの一例を示す図
【図２６】ニューロンの一例を示す図
【図２７】本発明の一実施例を示す図
【図２８】本発明の他の実施形態における窓口の構成を示す図
【図２９】本発明の他の実施形態における運用保守制御リストの更新確認画面の一例を示す図

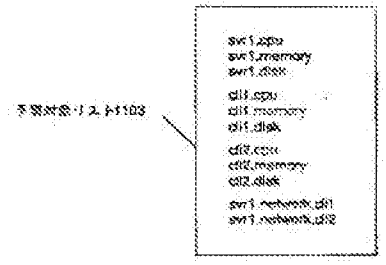
【図１】



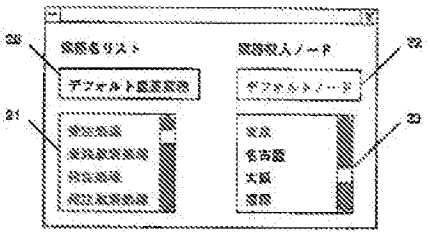
【図２】



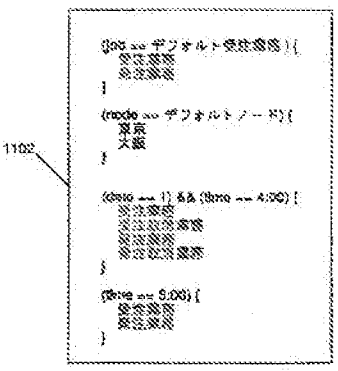
【図７】



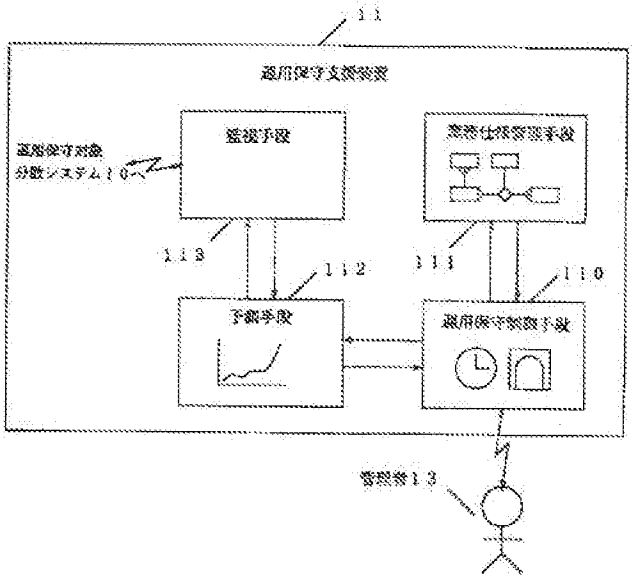
【図５】



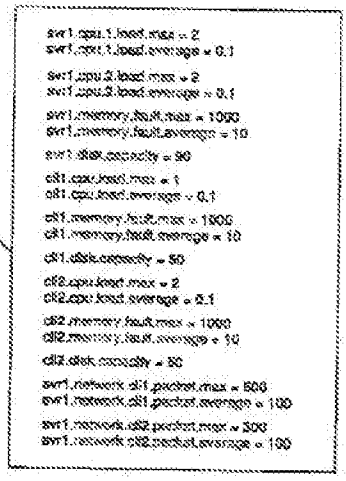
【図６】



【図3】



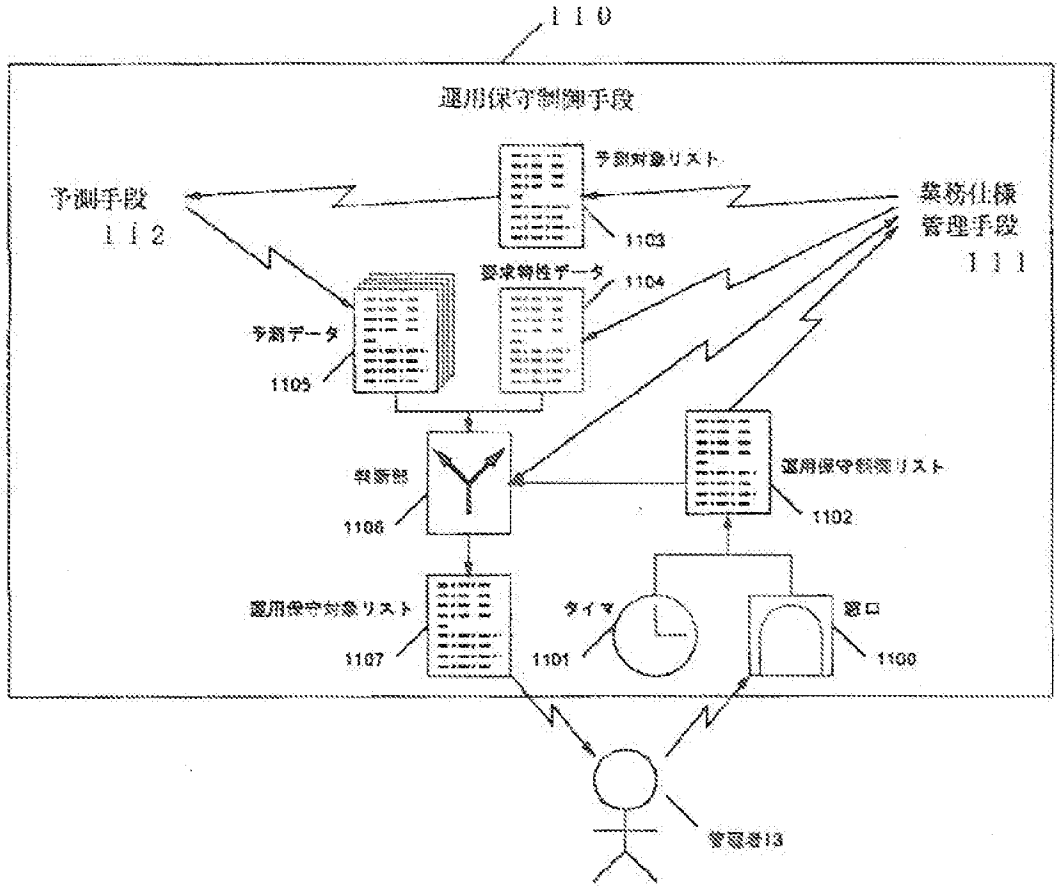
【図8】



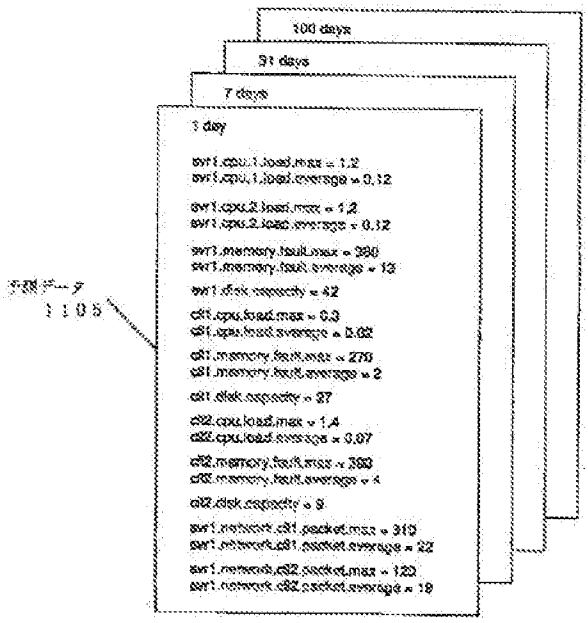
【図22】

ディスクID	空き容量情報
120	90%
121	80%
122	60%

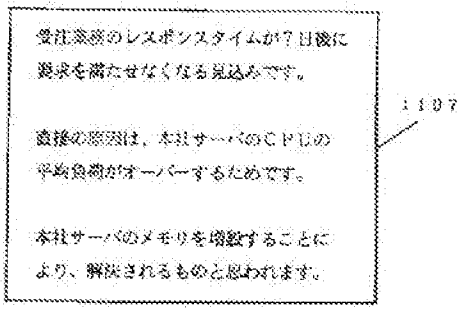
【図4】



【図9】



【図13】



【図16】

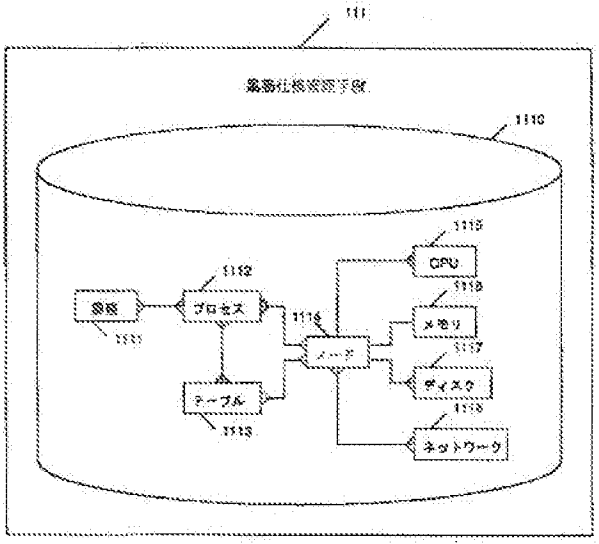
業務ID	業務名	レスポンスタイム
100	受注業務	3 sec
101	受注変更業務	5 sec
102	照会業務	7 sec
103	受注取消業務	7 sec

(A)

業務ID	プロセスID
100	100
100	101
100	102
101	100
101	103
102	100
102	104
102	105
103	100
103	105

(B)

【図15】



【図17】

(A)

プロセスID	プロセス名	処理時間	メモリ量
100	受注入力	10	500
101	変更	200	1000
102	照会	5	30
103	受注取消	500	750
104	発注	450	1000
105	受注取消	750	750

(B)

プロセスID	ノードID
100	clt1
100	clt2
101	svr1
102	clt1
102	clt2
103	svr1
104	svr1
105	svr1

(C)

プロセスID	テーブルID	ノードID
101	100	svr1
103	100	svr1
104	101	svr1
105	101	svr1

【図18】

テーブルID	テーブル名	レコードサイズ
100	受注	1024
101	商品	1280

(A)

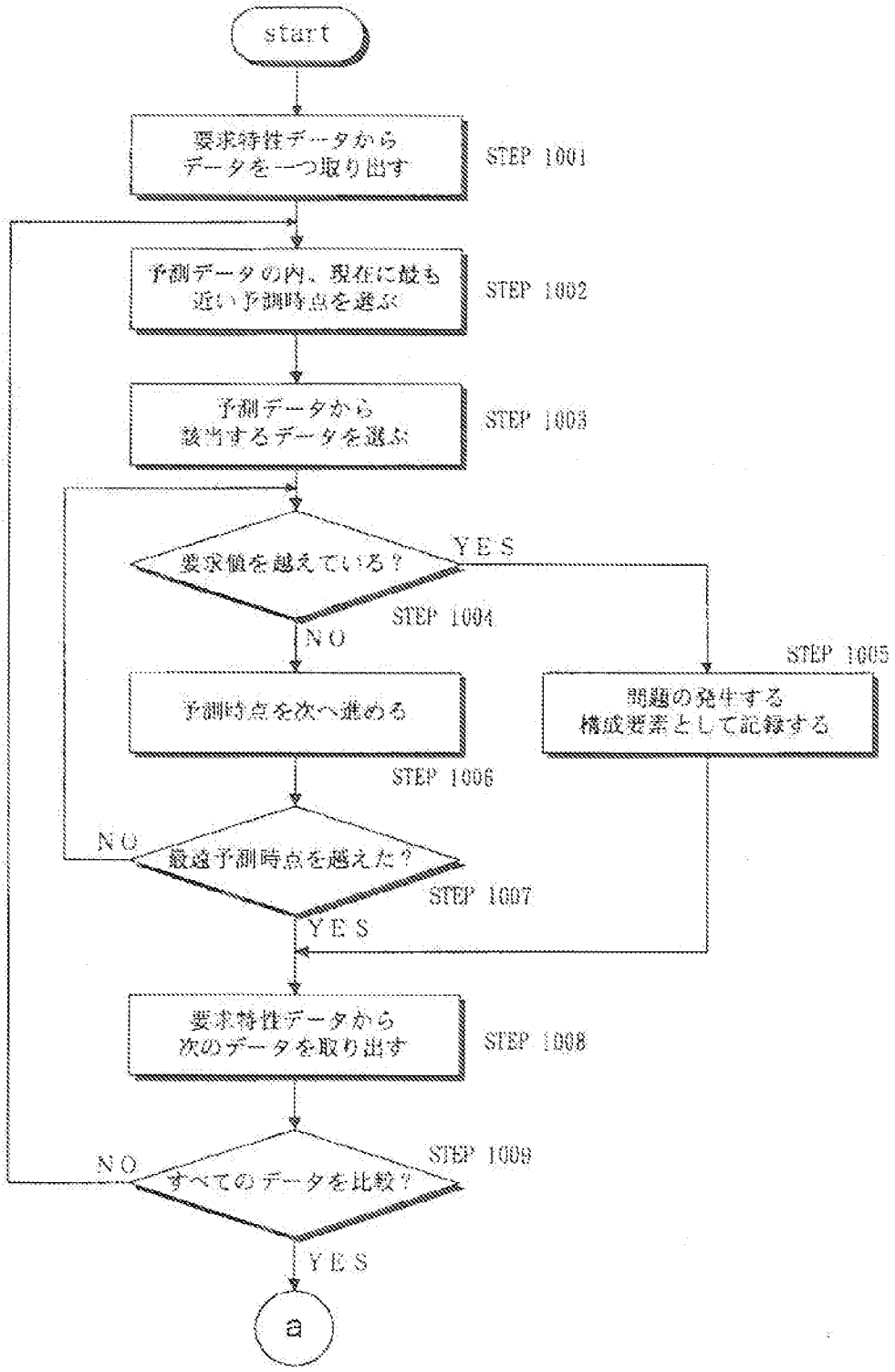
テーブルID	ノードID
100	svr1
101	svr1

(B)

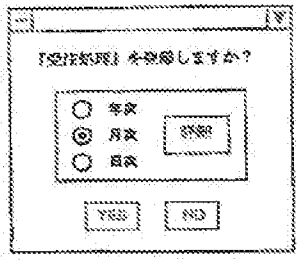
【図20】

CPUID	物理ID	最大負荷	平均負荷
100	0	2	0.1
101	2	2	0.1
102	1	1	0.3
103	1	2	0.1

【図10】



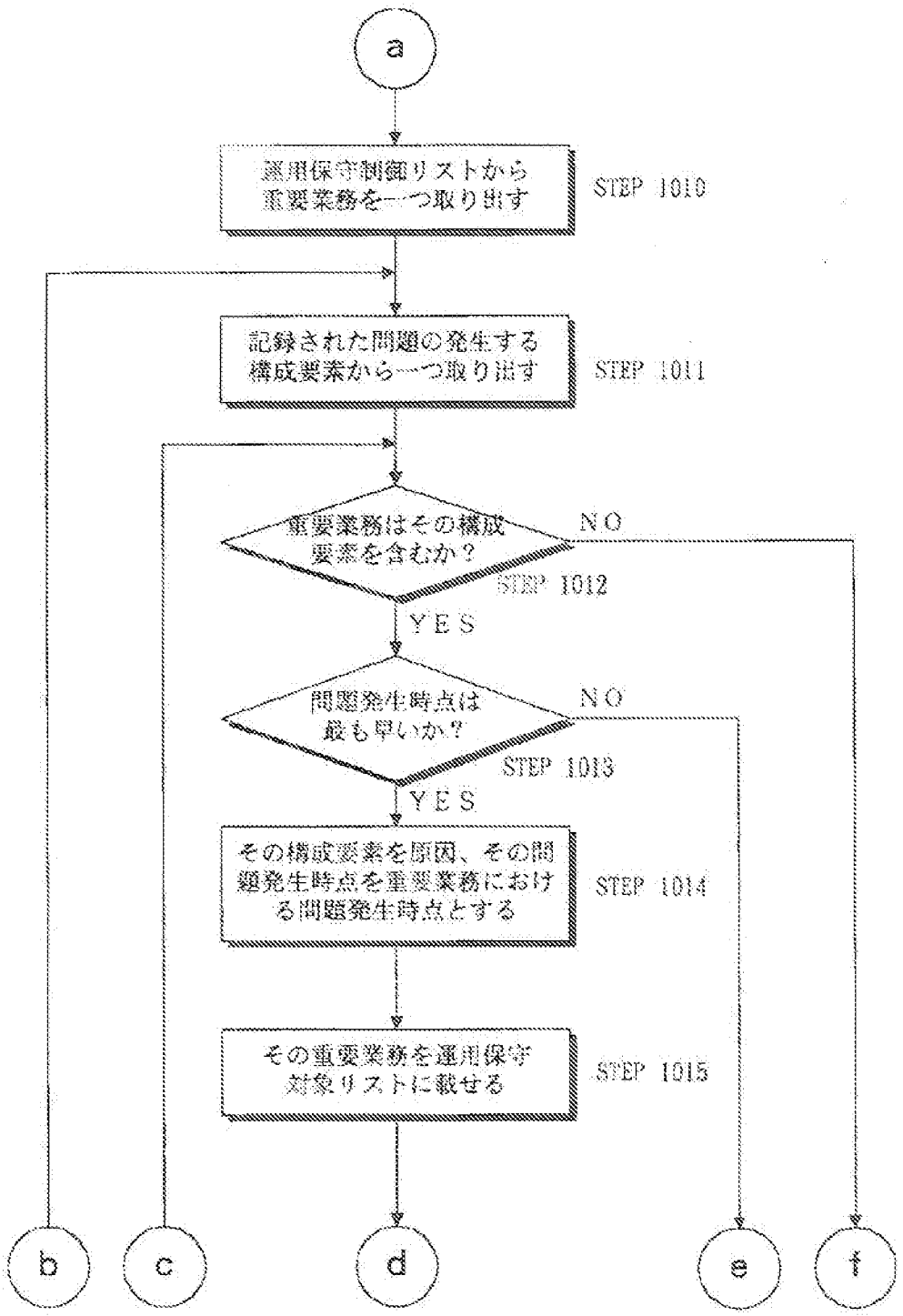
【図29】



【図23】

ネットワークID	ノードID1	ノードID2	送信パケット数	受信パケット数
100	ee1	ee1	5000	5000
100	ee1	ee2	3000	3000

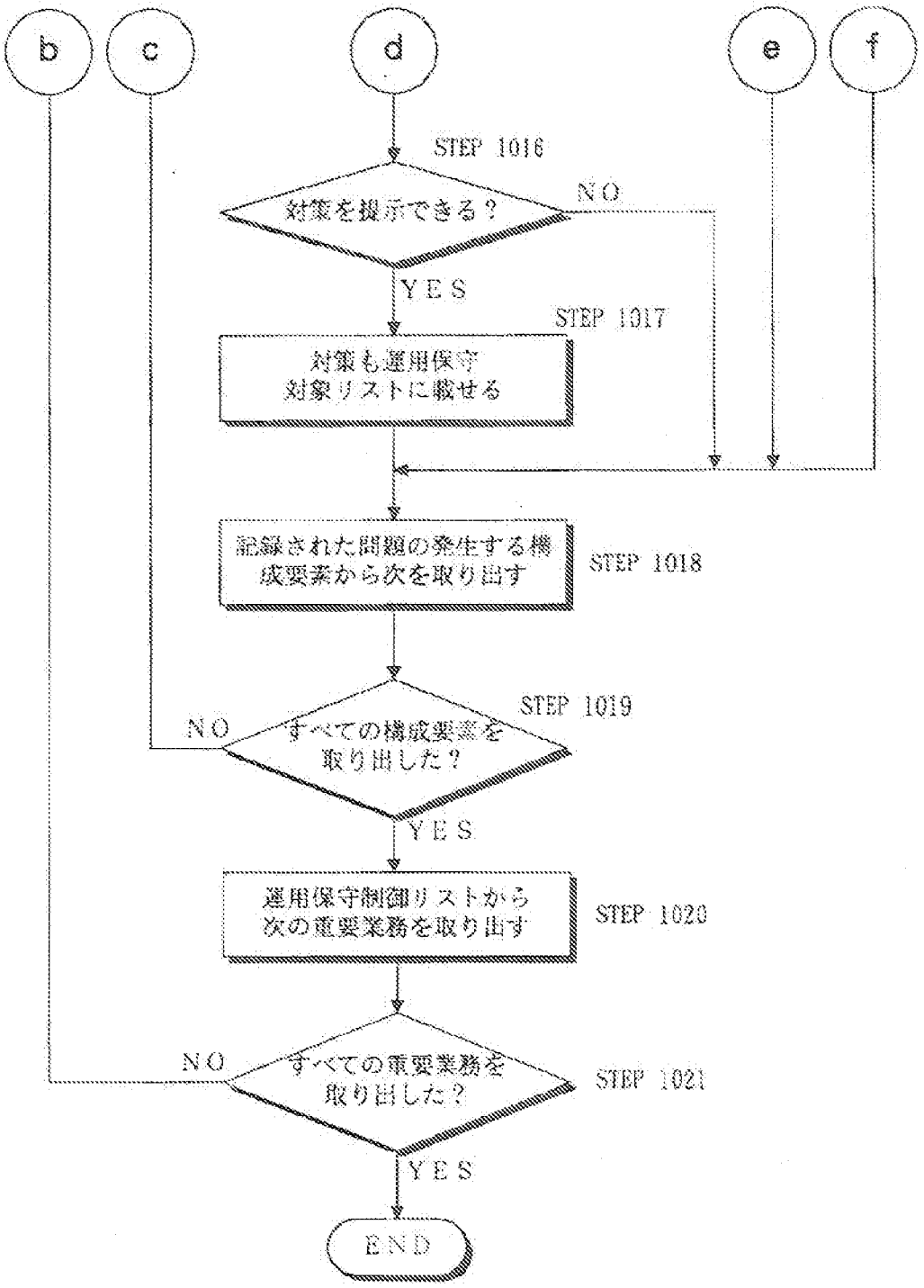
【図11】



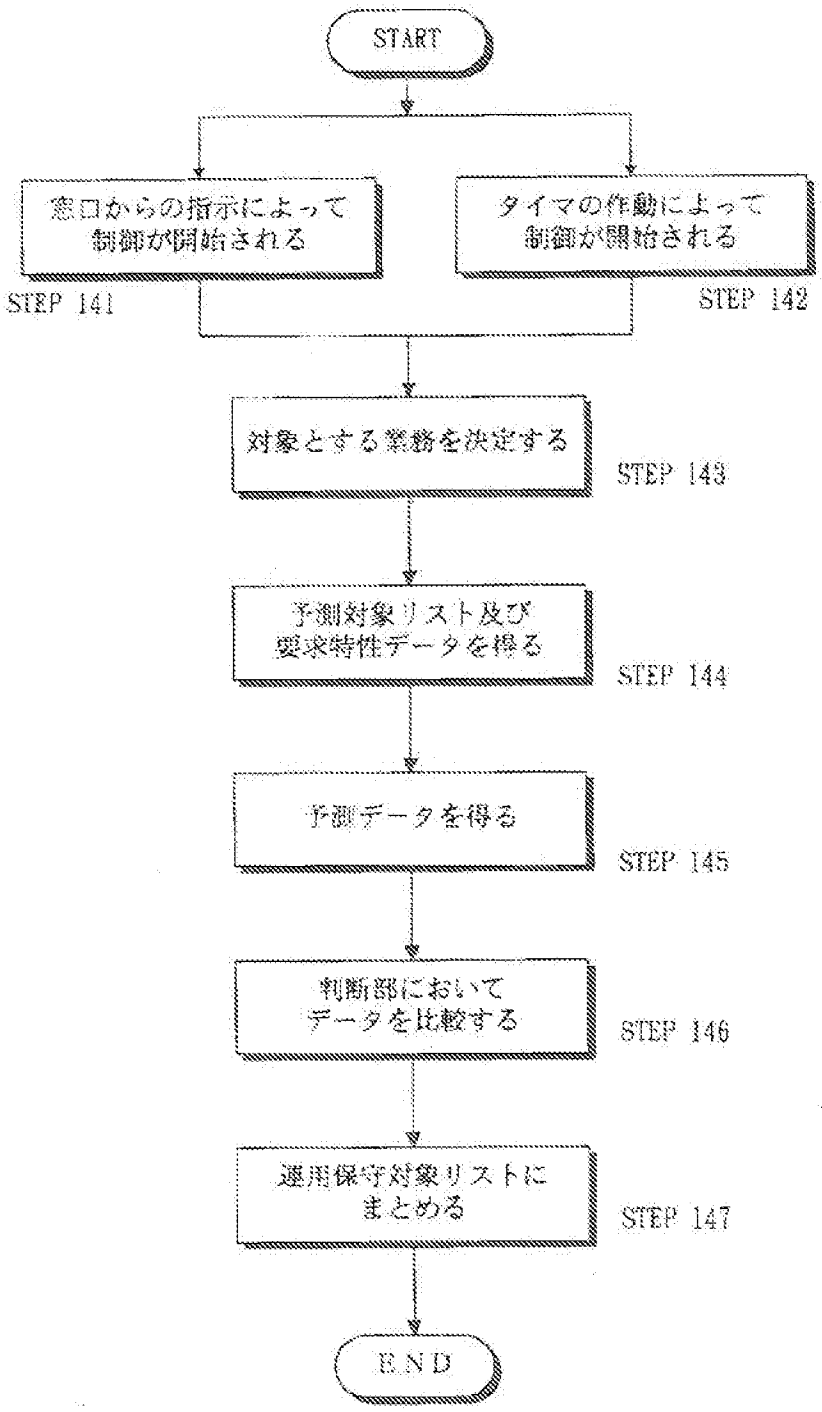
【図21】

メモリID	最大ページフォールト数	平均ページフォールト数
100	1000	10
101	1000	10
102	1000	10

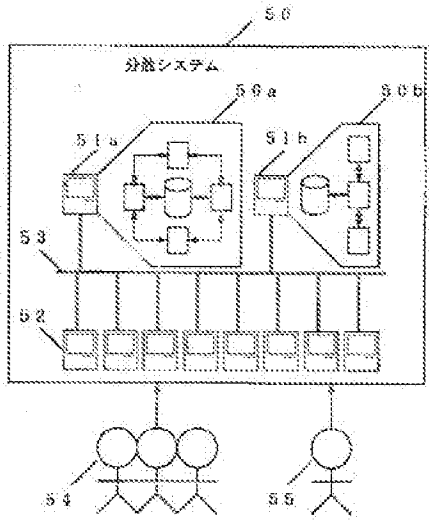
【図12】


b
c
d
e
f
STEP 1016
対策を提示できる？
NO
YES
STEP 1017
対策も運用保守
対象リストに載せる
記録された問題の発生する構
成要素から次を取り出す
STEP 1018
STEP 1019
NO
すべての構成要素を
取り出した？
YES
運用保守制御リストから
次の重要業務を取り出す
STEP 1020
NO
すべての重要業務を
取り出した？
STEP 1021
YES
END

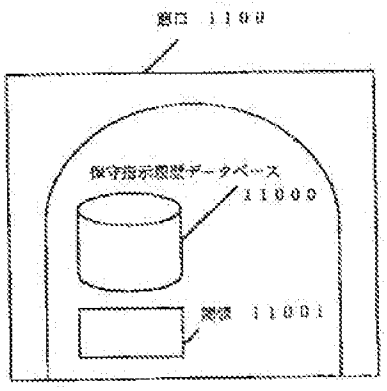
【図14】


START
窓口からの指示によって
制御が開始される
タイマの作動によって
制御が開始される
STEP 141
STEP 142
対象とする業務を決定する
STEP 143
予測対象リスト及び
要求特性データを得る
STEP 144
予測データを得る
STEP 145
判断部において
データを比較する
STEP 146
運用保守対象リストに
まとめる
STEP 147
END

【図27】


50
分散システム
50a
50b
51a
51b
53
52
54
55

【図28】


窓口 1100
保守指示関連データベース
11000
業務 11001

【図19】

(A)

ノードID	ノード名
svr1	本社
db1	営業
db2	大阪

(B)

ノードID	CPU ID
svr1	100
svr1	101
db1	102
db2	103

(C)

ノードID	メモリID
svr1	100
db1	101
db2	102

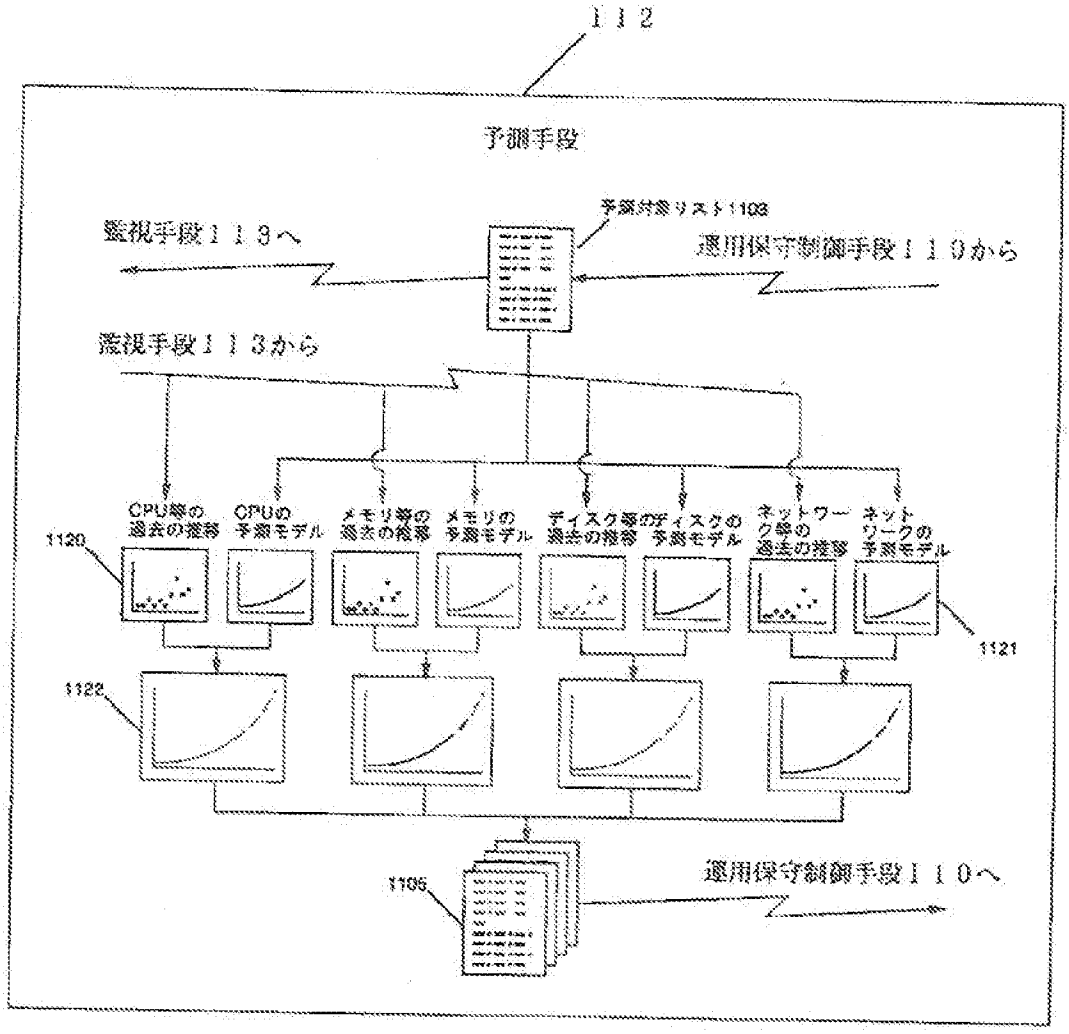
(D)

ノードID	ディスクID
svr1	100
db1	101
db2	102

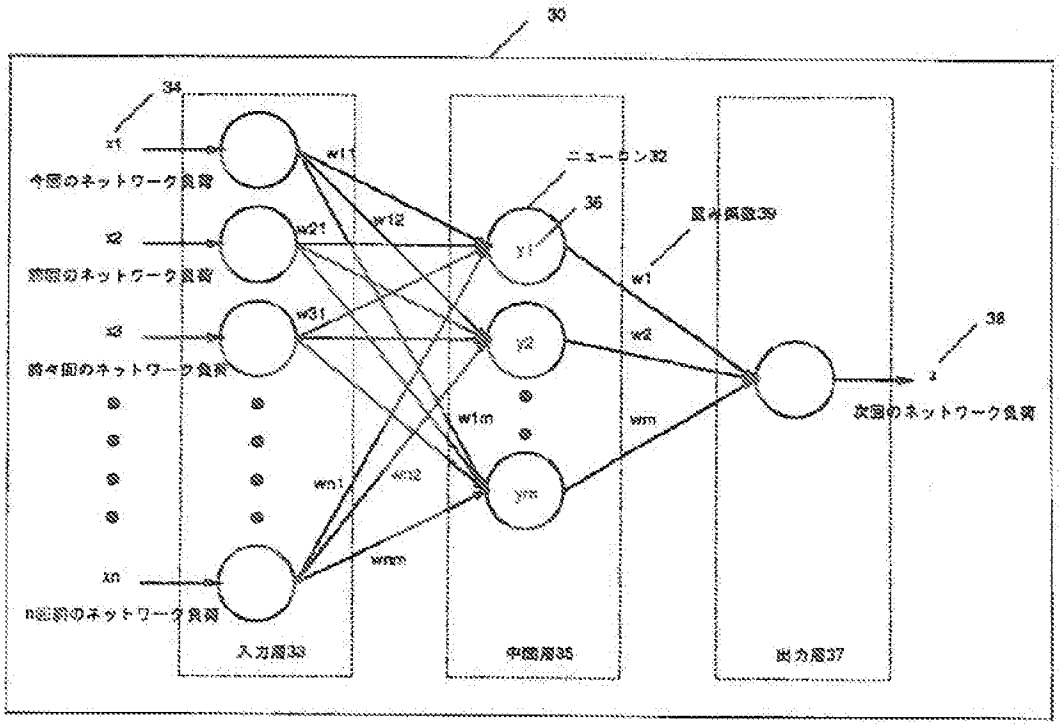
(E)

ノードID	ネットワークID
svr1	100
db1	101
db2	102

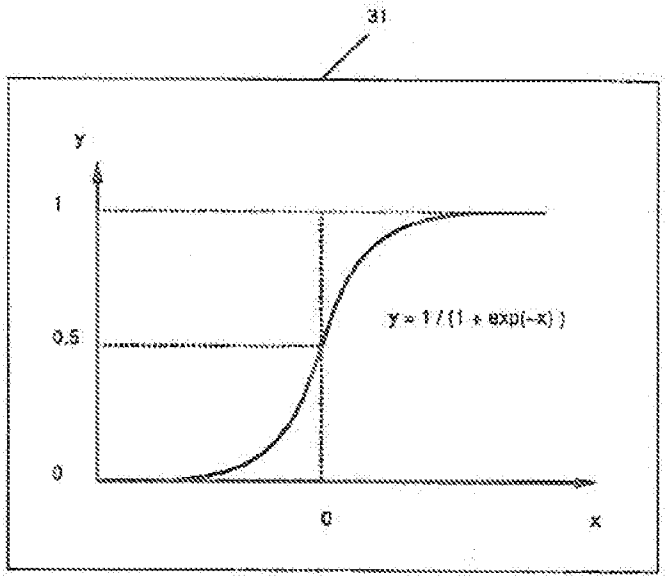
【図24】



【図25】


30
34
x1
今回のネットワーク負荷
x2
前回のネットワーク負荷
x3
前々回のネットワーク負荷
xn
n回前のネットワーク負荷
w11
w21
w31
wn1
w12
w13
wnm
ニューロン32
36
y1
y2
ym
w1m
wm
重み係数39
w1
w2
38
z
次回のネットワーク負荷
入力層33
中間層35
出力層37

【図26】


31
y
1
0.5
0
y = 1 / (1 + exp(-x))
0
x